

Configuration de vRealize Automation

15 mars 2018

vRealize Automation 7.3



vmware®

Vous trouverez la documentation technique la plus récente sur le site Web de VMware à l'adresse :

<https://docs.vmware.com/fr/>

N'hésitez pas à nous transmettre tous vos commentaires concernant cette documentation à l'adresse suivante :

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware, Inc.
100-101 Quartier Boieldieu
92042 Paris La Défense
France
www.vmware.com/fr

Copyright © 2015–2018 VMware, Inc. Tous droits réservés. [Copyright et informations sur les marques.](#)

Table des matières

Configuration de vRealize Automation 6

Informations mises à jour 7

1 Préparations externes pour le provisionnement de Blueprint 8

Préparation de votre environnement pour la gestion de vRealize Automation 8

Liste de vérification pour la préparation de la configuration du réseau et de la sécurité de NSX 10

Liste de contrôle pour assurer la prise en charge d'un fournisseur IPAM tiers 15

Liste de contrôle pour configurer Conteneurs pour vRealize Automation 19

Préparation de votre environnement vCloud Director pour vRealize Automation 20

Préparation de votre environnement vCloud Air pour vRealize Automation 21

Préparation de votre environnement Amazon AWS 21

Préparation des fonctionnalités Réseau et sécurité de Red Hat OpenStack 28

Préparation de votre environnement SCVMM 29

Configurer la connectivité VPC entre le réseau et Azure 30

Préparation du provisionnement de machines 32

Choix d'une méthode de provisionnement de machine à préparer 32

Liste de contrôle pour l'exécution de scripts Visual Basic lors du provisionnement 36

Utilisation d'un agent invité vRealize Automation dans un provisionnement 38

Liste de vérification pour la préparation du provisionnement par le clonage 46

Préparation pour le provisionnement vCloud Air et vCloud Director 61

Préparation du provisionnement Kickstart Linux 62

Préparation du provisionnement SCCM 65

Préparation du provisionnement de WIM 67

Préparation du provisionnement de l'image de machine virtuelle 75

Préparation du provisionnement de l'image de la machine Amazon 75

Scénario : préparation de ressources vSphere pour le provisionnement de machines dans
Rainpole 78

Préparation du provisionnement Logiciel 81

Préparation du provisionnement de machines avec Logiciel 82

Scénario : préparer un modèle vSphere CentOS pour les Blueprints de la machine clonée et du
composant logiciel 86

Scénario : Préparer l'importation du Blueprint de l'exemple d'application Dukes Bank pour
vSphere 90

2 Préparations de ressources et de locataires pour le provisionnement de Blueprints 95

Configuration des paramètres de locataire	95
Choix des options de configuration de Directories Management	96
Mise à niveau de connecteurs externes de gestion des répertoires	163
Scénario : configurer un lien Active Directory pour une instance hautement disponible de vRealize Automation	171
Configurez les connecteurs externes pour la carte à puce et l'authentification à des fournisseur d'identité tiers dans vRealize Automation	174
Créer un lien Active Directory à domaines multiples ou à forêts multiples	181
Configuration de groupes et de rôles d'utilisateur	183
Créer des locataires supplémentaires	188
Suppression d'un locataire	191
Configuration de la personnalisation	191
Liste de contrôle de la configuration des notifications	194
Créer un fichier Remote Desktop Protocol (RDP) personnalisé pour prendre en charge les connexions RDP des machines provisionnées	206
Scénario : ajouter des emplacements de centre de données pour des déploiements inter-région	206
Configuration de vRealize Orchestrator	208
Configuration des ressources	213
Liste de contrôle pour la configuration de ressources IaaS	213
Configuration des ressources XaaS	342
Création et configuration de conteneurs	353
Installation de plug-ins supplémentaires sur le serveur vRealize Orchestrator par défaut	375
Utilisation de stratégies Active Directory	376

3 Fourniture de Blueprints de service aux utilisateurs 380

Conception de Blueprints	380
Exportation et importation de Blueprints et de contenu	382
Scénario : Importer l'exemple d'application Dukes Bank pour vSphere et le configurer pour votre environnement	384
Scénario : test de l'exemple d'application Dukes Bank	388
Création d'une bibliothèque de conceptions	390
Conception de Blueprints de machine	392
Conception de composants Logiciel	482
Conception de Blueprints XaaS et d'actions sur les ressources	495
Publication d'un Blueprint	559
Assemblage de Blueprints composites	560
Description du comportement d'un Blueprint imbriqué	562
Sélection d'un composant de machine qui prend en charge des composants Logiciel	565
Création de liaisons de propriétés entre des composants de Blueprint	566

Création de dépendances explicites et contrôle de l'ordre de provisionnement	567
Gestion du catalogue de services	568
Liste de contrôle pour la configuration du catalogue de services	569
Création d'un service	570
Utilisation d'éléments du catalogue et d'actions	573
Création de droits	576
Utilisation de stratégies d'approbation	584
Demander le provisionnement de machine à l'aide d'un Blueprint paramétré	613
Scénario : mettre le Blueprint d'application CentOS avec MySQL à disposition dans le catalogue de services	615
Gestion des éléments de catalogue déployés	619
Exécution d'actions pour des ressources provisionnées	619
Spécifiez les paramètres de reconfiguration de machine et les éléments à prendre en compte pour la reconfiguration	643
Reconfigurer un équilibrage de charge dans un déploiement	651
Modifier les règles NAT dans un déploiement	652
Ajouter ou supprimer des éléments de sécurité dans un déploiement	653
Afficher toutes les règles NAT pour un dispositif NSX Edge existant	654

Configuration de vRealize Automation

Configuration de vRealize Automation fournit des informations relatives à la configuration de vRealize Automation et de vos environnements externes pour les préparer pour le provisionnement et la gestion de catalogue de vRealize Automation.

Public visé

Ces informations s'adressent aux professionnels de l'informatique responsables de la configuration de l'environnement vRealize Automation et aux administrateurs d'infrastructure responsables de la préparation des éléments dans l'infrastructure existante en vue d'un provisionnement dans vRealize Automation. Elles sont destinées aux administrateurs système Windows et Linux expérimentés qui maîtrisent les technologies de machine virtuelle et les opérations de centre de données.

Glossaire VMware Technical Publications

VMware Technical Publications fournit un glossaire des termes qui peuvent éventuellement ne pas vous être familiers. Pour consulter la définition des termes utilisés dans la documentation technique VMware, visitez le site Web <http://www.vmware.com/support/pubs>.

Informations mises à jour

Le tableau suivant répertorie les modifications apportées au guide *Configuration de vRealize Automation* pour la version de ce produit.

Révision	Description
15 mars 2018	<ul style="list-style-type: none">■ Mise à jour de Dépannage des problèmes de positionnement de la charge de travail pour inclure le nom du fichier journal.■ Mise à jour des scripts téléchargeables dans Préparer une machine de référence Windows pour prendre en charge Logiciel et Préparer une machine de référence Linux pour prendre en charge Logiciel.■ Mise à jour de la section Forcer la destruction d'un déploiement après l'échec d'une demande de destruction.■ Mises à jour mineures de Configurer un lien Active Directory utilisant le protocole LDAP/IWA.
18 janvier 2018	<ul style="list-style-type: none">■ Mise à jour de Configurez les connecteurs externes pour la carte à puce et l'authentification à des fournisseur d'identité tiers dans vRealize Automation pour rendre les informations plus génériques.
4 décembre 2017	Mises à jour mineures.
30 août 2017	<ul style="list-style-type: none">■ Configuration requise de l'administrateur pour le provisionnement d'objets universels NSX■ Rubrique Installer l'agent invité sur une machine de référence Windows mise à jour■ Mise à jour de la section Obtenir et importer un module de fournisseur IPAM tiers dans vRealize Orchestrator.■ Rôles d'utilisateur et informations d'identification Amazon AWS requis pour vRealize Automation
FR-002417-02	<ul style="list-style-type: none">■ Mise à jour de la section Installer le plug-in NSX sur vRealize Orchestrator.■ Mise à jour de la section Configurer un lien Active Directory utilisant le protocole LDAP/IWA.
FR-002417-01	<ul style="list-style-type: none">■ Mise à jour de la section Configurer un serveur vRealize Orchestrator externe.■ Mise à jour et ajout de liens vers l'article de la base de connaissances dans Éléments à prendre en compte lors de l'utilisation de points de terminaison mis à niveau ou migrés.■ Mise à jour de Scénario : Importer l'exemple d'application Dukes Bank pour vSphere pour résoudre un problème spécifique à la casse.■ Ajout d'un lien vers l'article de la base de connaissances dans Reconfigurer un équilibrage de charge dans un déploiement.■ Ajout d'une référence externe dans Création et utilisation de règles NAT.■ Ajout d'une référence externe dans Créer un point de terminaison NSX et l'associer à un point de terminaison vSphere.■ Mise à jour de la section Utilisation de propriétés de conteneur et de groupes de propriétés dans un Blueprint.
FR-002417-00	Version de document initiale.

Préparations externes pour le provisionnement de Blueprint

1

Vous pouvez avoir besoin de créer ou de préparer des éléments à l'extérieur de vRealize Automation pour prendre en charge le provisionnement d'éléments de catalogue. Par exemple, si vous souhaitez fournir un élément de catalogue pour le provisionnement d'une machine clonée, vous devez créer un modèle de clone sur votre hyperviseur.

Ce chapitre aborde les rubriques suivantes :

- [Préparation de votre environnement pour la gestion de vRealize Automation](#)
- [Configurer la connectivité VPC entre le réseau et Azure](#)
- [Préparation du provisionnement de machines](#)
- [Préparation du provisionnement Logiciel](#)

Préparation de votre environnement pour la gestion de vRealize Automation

En fonction de votre plate-forme d'intégration, certaines modifications de configuration peuvent être nécessaires avant de pouvoir implémenter la gestion de vRealize Automation ou avant de pouvoir exploiter certaines fonctionnalités.

Tableau 1-1. Préparation de votre environnement pour l'intégration de vRealize Automation







Environnement	Préparations
	<p>Si vous souhaitez tirer parti de NSX pour gérer les fonctionnalités de mise en réseau et de sécurité des machines provisionnées avec vRealize Automation, préparez votre instance de NSX pour intégration. Reportez-vous à Liste de vérification pour la préparation de la configuration du réseau et de la sécurité de NSX.</p>
 vCloud Director	<p>Installez et configurez l'instance de vCloud Director, configurez les ressources de vSphere et les ressources cloud, puis identifiez ou créez des informations d'identification appropriées pour fournir à vRealize Automation l'accès à l'environnement vCloud Director. Reportez-vous à Préparation de votre environnement vCloud Director pour vRealize Automation.</p>
 vCloud Air	<p>Enregistrez le compte vCloud Air, configurez l'environnement vCloud Air, puis identifiez ou créez des informations d'identification appropriées pour fournir à vRealize Automation l'accès à l'environnement. Reportez-vous à Préparation pour le provisionnement vCloud Air et vCloud Director.</p>
 Amazon AWS	<p>Préparez des éléments et des rôles d'utilisateurs dans votre environnement Amazon AWS à utiliser dans vRealize Automation et apprenez comment les fonctionnalités Amazon AWS se mappent aux fonctionnalités vRealize Automation. Reportez-vous à Préparation de votre environnement Amazon AWS.</p>
Microsoft Azure	<p>Configurez le réseau afin d'utiliser le tunneling VPN pour prendre en charge des composants logiciels sur des Blueprints Azure. Reportez-vous à Configurer la connectivité VPC entre le réseau et Azure.</p>
 Red Hat OpenStack	<p>Si vous souhaitez tirer parti de Red Hat OpenStack pour gérer les fonctionnalités de mise en réseau et de sécurité des machines provisionnées avec vRealize Automation, préparez votre instance de Red Hat OpenStack pour intégration. Reportez-vous à Préparation des fonctionnalités Réseau et sécurité de Red Hat OpenStack.</p>

Tableau 1-1. Préparation de votre environnement pour l'intégration de vRealize Automation (suite)

Environnement	Préparations
 SCVMM	Configurez le stockage et la mise en réseau, puis étudiez les restrictions de dénomination du profil matériel et du profil du modèle. Reportez-vous à Préparation de votre environnement SCVMM .
Fournisseurs IPAM externes	Enregistrez un module ou un plug-in de fournisseur IPAM externe, exécutez les workflows de configuration et enregistrez la solution IPAM en tant que nouveau point de terminaison vRealize Automation. Reportez-vous à Liste de contrôle pour assurer la prise en charge d'un fournisseur IPAM tiers .
Tous les autres environnements	Aucun changement n'est nécessaire. Vous pouvez commencer à préparer la machine pour provisionnement en créant des modèles, des environnements de démarrage ou des images de machine. Reportez-vous à Préparation du provisionnement de machines .

Liste de vérification pour la préparation de la configuration du réseau et de la sécurité de NSX

Avant que vous puissiez utiliser les options de réseau et de sécurité de NSX dans vRealize Automation, vous devez configurer l'environnement réseau et de sécurité externe de NSX que vous prévoyez d'utiliser.

À partir de vRealize Automation 7.3, vous n'avez plus besoin d'installer le plug-in NSX pour obtenir la fonctionnalité NSX intégrée. Toute la fonctionnalité NSX intégrée provient désormais directement des API NSX et non du plug-in NSX. Cependant, si vous souhaitez utiliser XaaS pour étendre votre intégration de vRealize Automation et de NSX, vous devez installer le plug-in NSX dans vRealize Orchestrator comme il est décrit ici.

En préparation de l'utilisation des capacités de réseau, de sécurité et d'équilibrage de charge NSX dans vRealize Automation, lors de l'utilisation des informations d'identification du gestionnaire NSX vous devez utiliser le compte d'administrateur gestionnaire NSX.

Pour obtenir des informations connexes sur NSX, consultez la documentation de NSX à l'adresse https://www.vmware.com/support/pubs/nsx_pubs.html et les blogs publics et articles tels que [Intégration de NSX à vRealize Automation](#).

La majeure partie de la prise en charge de vRealize Automation de la configuration du réseau et de la sécurité que vous spécifiez dans les Blueprints et les réservations est configurée en externe et rendue disponible pour vRealize Automation une fois la collecte de données exécutée sur les ressources de calcul.

Pour plus d'informations sur les paramètres NSX que vous pouvez configurer pour les Blueprints vRealize Automation, reportez-vous à la section [Configuration des paramètres de composants de réseau et de sécurité](#).

Tableau 1-2. Préparation de la liste de vérification du réseau et de la sécurité de NSX

Tâche	Emplacement	Détails
<input type="checkbox"/> Configurez les paramètres réseau NSX, y compris les paramètres de passerelle et de zone de transport.	Configurez les paramètres réseau dans NSX.	Reportez-vous au <i>Guide d'administration de NSX</i> .
<input type="checkbox"/> Créez des stratégies de sécurité, des balises et des groupes NSX.	Configurez les paramètres de sécurité dans NSX.	Reportez-vous au <i>Guide d'administration de NSX</i> .
<input type="checkbox"/> Configurez les paramètres d'équilibrage de charge NSX.	Configurez un équilibrage de charge NSX devant fonctionner avec vRealize Automation.	Reportez-vous au <i>Guide d'administration de NSX</i> . Reportez-vous également à la section Propriétés personnalisées pour la mise en réseau dans <i>Référence des propriétés personnalisées</i> .
<input type="checkbox"/> Pour les déploiements cross-vCenter, vérifiez que le dispositif NSX Manager de calcul détient le rôle principal.	Le provisionnement de vRealize Automation nécessite que le dispositif NSX Manager de calcul de la région dans laquelle réside les machines détienne le rôle principal.	Reportez-vous à Configuration requise de l'administrateur pour le provisionnement d'objets universels NSX . Reportez-vous au <i>Guide d'installation de NSX</i> et au <i>Guide d'administration de NSX</i> pour plus d'informations sur les déploiements cross-vCenter, les objets universels et le rôle de dispositif NSX Manager principal.

Installer le plug-in NSX sur vRealize Orchestrator

L'installation du plug-in NSX nécessite de télécharger le fichier d'installation de vRealize Orchestrator, d'utiliser l'interface de configuration de vRealize Orchestrator pour télécharger le fichier de plug-in et d'installer le plug-in sur un serveur vRealize Orchestrator.

Pour des informations d'ordre général sur la mise à jour et le dépannage des plug-ins, reportez-vous à la [documentation](#) de vRealize Orchestrator.

Prérequis

À partir de vRealize Automation 7.3, vous n'avez plus besoin d'installer le plug-in NSX pour obtenir la fonctionnalité NSX intégrée. Toute la fonctionnalité NSX intégrée provient désormais directement des API NSX et non du plug-in NSX. Cependant, si vous souhaitez utiliser XaaS pour étendre votre intégration de vRealize Automation et de NSX, vous devez installer le plug-in NSX dans vRealize Orchestrator comme il est décrit ici.

Si vous utilisez une instance intégrée de vRealize Orchestrator qui contient déjà un plug-in NSX installé, vous pouvez ignorer cette procédure.

- Vérifiez que vous exécutez une instance vRealize Orchestrator prise en charge.
Pour obtenir des informations sur la configuration de vRealize Orchestrator, reportez-vous à *Installation et configuration de VMware vRealize Orchestrator*.
- Vérifiez que vous disposez des informations d'identification d'un compte avec l'autorisation d'installer les plug-in vRealize Orchestrator et de s'authentifier par le biais de vCenter Single Sign-On.
- Vérifiez que vous avez installé le client vRealize Orchestrator et que vous pouvez vous connecter avec des informations d'identification d'administrateur.
- Vérifiez que la version du plug-in est la bonne NSX dans la [matrice de support](#) de vRealize Automation .

Procédure

- 1 Téléchargez le fichier de plug-in dans un emplacement accessible depuis le serveur vRealize Orchestrator.

Le format du nom du fichier d'installation de plug-in, avec les valeurs de version appropriées, est `o11nplugin-nsx-1.n.n.vmoapp`. Les fichiers d'installation du plug-in pour le produit de mise en réseau et de sécurité NSX sont disponibles sur le site de téléchargement du produit VMware à l'adresse <http://vmware.com/web/vmware/downloads>.

- 2 Ouvrez un navigateur et lancez l'interface de configuration de vRealize Orchestrator.
Un exemple de format de l'URL est `https://orchestrator_server.com:8283`.
- 3 Cliquez sur **Plug-Ins** dans le volet gauche et défilez jusqu'à la section Installer un nouveau plug-in.
- 4 Dans la zone de texte **Fichier de plug-In**, accédez au fichier d'installation du plug-in et cliquez sur **Télécharger et installer**.

Le fichier doit être dans le format `.vmoapp`.

- 5 À l'invite, acceptez le contrat de licence dans le volet Installer le plug-in.
- 6 Dans la section de l'état d'installation des plug-ins activés, confirmez que le nom spécifié du plug-in NSX est correct.

Consultez *Matrice de prise en charge de vRealize Automation* pour obtenir des d'informations sur la version.

Le statut Le plug-in sera installé au prochain démarrage du serveur s'affiche.

- 7 Redémarrez le service du serveur vRealize Orchestrator.
- 8 Redémarrez l'interface de configuration de vRealize Orchestrator.
- 9 Cliquez sur **Plug-Ins** et vérifiez que le statut est à présent **Installation OK**.
- 10 Démarrez l'application du client vRealize Orchestrator, connectez-vous et utilisez l'onglet **Workflow** pour rechercher dans la bibliothèque le dossier NSX.

Vous pouvez parcourir les workflows fournis par le plug-in NSX.

Suivant

Créez un point de terminaison vRealize Orchestrator dans vRealize Automation qui sera utilisé pour exécuter les workflows. Reportez-vous à [Créez un point de terminaison vRealize Orchestrator](#).

Exécuter un workflow de sécurité vRealize Orchestrator et NSX

Pour que vous puissiez utiliser les NSX fonctionnalités de stratégie de sécurité vRealize Automation, un administrateur doit au préalable exécuter le workflow `Enable security policy support for overlapping subnets` dans vRealize Orchestrator.

La prise en charge de la stratégie de sécurité pour les sous-réseaux qui se chevauchent s'applique uniquement à un point de terminaison NSX 6.1 et version ultérieure. N'exécutez ce workflow qu'une seule fois pour activer cette prise en charge.

Prérequis

- Vérifiez qu'un point de terminaison vSphere est inscrit avec un point de terminaison NSX. Reportez-vous à [Créer un point de terminaison vSphere](#).
- Connectez-vous au client vRealize Orchestrator en tant qu'administrateur.
- Vérifiez que vous avez exécuté le workflow `vRO Create NSX endpoint`.

Procédure

- 1 Cliquez sur l'onglet **Workflow** et sélectionnez **NSX > Workflows NSX pour VCAC**.
- 2 Exécutez le workflow **Créer un point de terminaison NSX** et répondez aux invites.
- 3 Exécutez le workflow **Activer la prise en charge de la stratégie de sécurité pour les sous-réseaux qui se chevauchent**.
- 4 Sélectionnez le point de terminaison NSX comme paramètre d'entrée pour le workflow.

Utilisez l'adresse IP que vous avez spécifiée lors de la création du point de terminaison vSphere pour enregistrer une instance NSX.

Une fois que vous avez exécuté ce workflow, les règles de pare-feu distribué définies dans la stratégie de sécurité sont appliquées uniquement aux cartes réseau virtuelles des membres du groupe de sécurité auxquels cette stratégie de sécurité est appliquée.

Suivant

Appliquez les fonctionnalités de sécurité applicables dans le Blueprint.

Configuration requise de l'administrateur pour le provisionnement d'objets universels NSX

Pour provisionner des machines dans un environnement vCenter NSX lors de l'utilisation d'objets universels NSX, vous devez provisionner dans une instance de vCenter dans laquelle le gestionnaire de calcul NSX a le rôle principal.

Dans un environnement vCenter NSX, il est possible d'avoir plusieurs instances de vCenter Server, chacune devant être associée à sa propre instance de NSX Manager. Une instance de NSX Manager obtient le rôle de NSX Manager principal, et les autres le rôle de NSX Manager secondaire.

L'instance principale de NSX Manager peut créer des objets universels, par exemple des commutateurs logiques universels. Ces objets sont synchronisés avec les instances secondaires de NSX Manager. Vous pouvez afficher ces objets à partir des instances secondaires de NSX Manager, mais vous ne pouvez pas les y modifier. Pour gérer les objets universels, vous devez utiliser l'instance principale de NSX Manager. Vous pouvez utiliser l'instance principale de NSX Manager pour configurer n'importe quelle instance secondaire de NSX Manager dans l'environnement.

Pour plus d'informations sur l'environnement vCenter NSX, reportez-vous à *Présentation de la mise en réseau et de la sécurité vCenter* dans le *Guide d'administration de NSX* de la [documentation du produit NSX](#).

Pour un point de terminaison vSphere (vCenter) qui est associé au point de terminaison NSX d'une instance principale de NSX Manager, vRealize Automation prend en charge les objets locaux NSX, tels que des commutateurs logiques locaux, les passerelles Edge locales, les équilibrages de charge locaux, les groupes de sécurité et les balises de sécurité. Il prend également en charge les réseaux NAT un-à-un et un-à-plusieurs avec zone de transport universelle, les réseaux acheminés avec zone de transport universelle et les routeurs logiques distribués (DLR) universels et un équilibrage de charge avec n'importe quel type de réseau.

vRealize Automation ne prend pas en charge les groupes de sécurité universelle existants et à la demande ou les balises NSX.

Pour provisionner des réseaux à la demande, en tant qu'instance principale de NSX, utilisez une zone de transport locale spécifique à vCenter. Vous pouvez configurer des réservations vRealize Automation pour utiliser la zone de transport locale et des câbles virtuels pour des déploiements dans cette instance locale de vCenter.

Si vous connectez un point de terminaison vSphere (vCenter) à un point de terminaison d'une instance secondaire correspondante de NSX Manager, vous pouvez uniquement provisionner et utiliser des objets locaux.

Vous pouvez uniquement associer un point terminaison NSX à un point de terminaison vSphere. Cette contrainte d'association signifie que vous ne pouvez pas provisionner un réseau à la demande universel et l'attacher aux machines vSphere provisionnées sur différents serveurs vCenter.

vRealize Automation peut utiliser un commutateur logique universel NSX comme réseau externe. Si un commutateur universel existe, ses données sont collectées et il est attaché ou consommé par chaque machine du déploiement.

- Le provisionnement d'un réseau à la demande dans une zone de transport universelle peut créer un nouveau commutateur logique universel.
- Le provisionnement d'un réseau à la demande dans une zone de transport universelle sur l'instance principale de NSX Manager crée un commutateur logique universel.
- Le provisionnement d'un réseau à la demande dans une zone de transport universelle sur une instance secondaire de NSX Manager échoue, car NSX ne peut pas créer un commutateur logique universel sur une instance secondaire de NSX Manager.

Consultez l'article de la base de connaissances VMware *Le déploiement de Blueprints vRealize Automation avec des objets NSX échoue (2147240)* à l'adresse <http://kb.vmware.com/kb/2147240> pour plus d'informations sur les objets universels NSX.

Liste de contrôle pour assurer la prise en charge d'un fournisseur IPAM tiers

Vous pouvez obtenir des adresses IP et des plages à utiliser dans la définition du profil réseau d'un fournisseur IPAM tiers pris en charge, tel qu'Infoblox.

Avant de pouvoir créer et utiliser un point de terminaison de fournisseur IPAM externe dans un profil réseau vRealize Automation, vous devez télécharger ou obtenir un plug-in ou module de fournisseur IPAM vRealize Orchestrator, importer le plug-in ou module, puis exécuter les workflows requis dans vRealize Orchestrator et enregistrer la solution IPAM en tant que point de terminaison vRealize Automation.

Pour accéder à la présentation du processus de provisionnement pour utiliser un fournisseur IPAM externe afin de fournir une plage d'adresses IP possibles, reportez-vous à [Provisionnement d'un déploiement vRealize Automation à l'aide d'un fournisseur IPAM tiers](#).

Tableau 1-3. Liste de contrôle pour la préparation de la prise en charge du fournisseur IPAM externe

Tâche	Description	Détails
<input type="checkbox"/> Obtenir et importer le plug-in vRealize Orchestrator du fournisseur IPAM externe pris en charge.	<p>Téléchargez le plug-in ou le module du fournisseur IPAM (par exemple, le plug-in appelé Plug-in Infoblox IPAM pour vRealize Orchestrator) et sa documentation à partir de VMware Solution Exchange (https://solutionexchange.vmware.com/store/category_group/s/cloud-management), puis importez le plug-in ou le module dans vRealize Orchestrator.</p> <p>Si VMware Solution Exchange ne contient pas le module du fournisseur IPAM dont vous avez besoin, vous pouvez créer votre propre module en utilisant le kit de développement logiciel d'un fournisseur de solutions IPAM tiers et la documentation connexe.</p> <p>Un kit de développement logiciel du fournisseur de solutions IPAM tiers spécifique à la version de vRealize Automation, sa documentation connexe et le module de démarrage associé pour vRealize Orchestrator et vRealize Automation sont disponibles sur https://code.vmware.com/sdks ou https://code.vmware.com/samples.</p>	<p>Reportez-vous à Obtenir et importer un module de fournisseur IPAM tiers dans vRealize Orchestrator.</p>
<input type="checkbox"/> Exécutez les workflows de configuration requis et enregistrez la solution IPAM externe en tant que point de terminaison vRealize Automation.	<p>Exécutez les workflows de configuration vRealize Orchestrator et enregistrez le type de point de terminaison du fournisseur IPAM dans vRealize Orchestrator.</p>	<p>Reportez-vous à Exécuter un workflow pour enregistrer un type de point de terminaison IPAM tiers dans vRealize Orchestrator.</p>

Obtenir et importer un module de fournisseur IPAM tiers dans vRealize Orchestrator

Pour préparer la définition et l'utilisation d'un point de terminaison de fournisseur IPAM tiers, vous devez d'abord obtenir le module du fournisseur IPAM tiers et l'importer dans vRealize Orchestrator.

Vous pouvez télécharger et utiliser un plug-in de fournisseur de gestion d'adresses IP tiers, par exemple Infoblox IPAM. Vous pouvez également créer votre propre plug-in ou module IPAM tiers à l'aide du module de démarrage fourni par VMware et de la documentation SDK connexe, à utiliser avec un autre fournisseur de solution IPAM tiers tel que Bluecat.

- Obtenez le plug-in et la documentation depuis [Infoblox IPAM Plug-in for vRealize Orchestrator](#) sur marketplace.vmware.com. Le téléchargement contient également la documentation relative à l'installation et à l'utilisation du plug-in.

- Créez votre propre solution IPAM tiers en obtenant et en utilisant un SDK du fournisseur de solutions IPAM tiers, la documentation connexe et un module de démarrage associé pour vRealize Orchestrator et vRealize Automation depuis code.vmware.com/web/sdk sur la page [vRealize Automation Third-Party IPAM Integration SDK 7.3](#).

Après avoir importé le plug-in ou le module de fournisseur IPAM tiers dans vRealize Orchestrator, vous devez exécuter les workflows requis et enregistrer le type de point de terminaison IPAM dans vRealize Orchestrator.

Pour plus d'informations sur l'importation de plug-ins et modules et l'exécution de workflows vRealize Orchestrator, reportez-vous à la section *Utilisation du client VMware vRealize Orchestrator*. Pour plus d'informations sur l'extension de vRealize Automation avec les plug-ins, modules et workflows vRealize Orchestrator, reportez-vous à *Extensibilité du cycle de vie*.

Cette séquence d'étapes utilise le plug-in Infoblox IPAM en tant qu'exemple. Votre séquence d'étapes peut varier en fonction de votre version de vRealize Automation ou de plug-in.

Prérequis

- Téléchargez le module ou plug-in à partir de marketplace.vmware.com.
- Connectez-vous à vRealize Orchestrator avec des privilèges d'administrateur pour importer, configurer et enregistrer un plug-in ou module vRealize Orchestrator.

Procédure

1 Ouvrez le site marketplace.vmware.com.

2 Localisez et téléchargez le plug-in ou le module.

Par exemple, importez le plug-in Infoblox prenant en charge le point de terminaison IPAM tiers Infoblox dans vRealize Orchestrator et vRealize Automation 7.1, et versions ultérieures.

- Dans la catégorie **Éditeur**, sélectionnez **Infoblox** et cliquez sur **Appliquer**.
- Sélectionnez [The Infoblox Plug-in for vRealize Orchestrator](#).
- Cliquez sur **Caractéristiques techniques** et étudiez les conditions préalables.
- Cliquez sur **Essayer** pour obtenir des informations complémentaires et pour recevoir un e-mail contenant un lien vers le téléchargement.
- Téléchargez le fichier zip comme spécifié dans les instructions de l'e-mail.

La version 4.0 et les versions ultérieures du plug-in prennent en charge vRealize Automation 7.1 et ses versions ultérieures. Le fichier zip contient également une documentation sur le plug-in.

3 Dans vRealize Orchestrator, cliquez sur l'onglet **Administrator**, puis cliquez sur **Import package**.

4 Sélectionnez le module à importer.

5 Sélectionnez tous les workflows et artefacts, puis cliquez sur **Importer les éléments sélectionnés**.

Suivant

[Exécuter un workflow pour enregistrer un type de point de terminaison IPAM tiers dans vRealize Orchestrator.](#)

Exécuter un workflow pour enregistrer un type de point de terminaison IPAM tiers dans vRealize Orchestrator

Exécutez le workflow d'enregistrement dans vRealize Orchestrator pour prendre en charge l'utilisation par vRealize Automation du fournisseur IPAM tiers et enregistrez le type de point de terminaison IPAM à utiliser dans vRealize Automation.

Pour enregistrer les types de point de terminaison IPAM dans vRealize Orchestrator, vous êtes invité à fournir les informations d'identification d'administrateur de vRealize Automation vRA.

Pour plus d'informations sur l'importation de modules et l'exécution de workflows de vRealize Orchestrator, reportez-vous à la section *Utilisation du client VMware vRealize Orchestrator*. Pour plus d'informations sur l'extension de vRealize Automation avec les modules et workflows vRealize Orchestrator, reportez-vous à *Extensibilité du cycle de vie*.

Prérequis

- [Obtenir et importer un module de fournisseur IPAM tiers dans vRealize Orchestrator](#)
- Vérifiez que vous êtes connecté à vRealize Orchestrator avec vRealize Automation avec autorité pour exécuter les workflows.
- Préparez-vous à fournir les informations d'identification d'administrateur vRealize Automation vRealize Automation lorsque vous y êtes invité.

Procédure

- 1 Dans vRealize Orchestrator, cliquez sur l'onglet **Conception**, sélectionnez **Administrateur > Bibliothèque** et sélectionnez **SDK du module de service IPAM**.

Chaque module de fournisseur IPAM dispose d'un nom unique et contient des workflows uniques. Chaque fournisseur fournit son propre workflow d'enregistrement. Tandis que les noms de workflow peuvent être similaires entre les modules de fournisseur, l'emplacement des workflows dans vRealize Orchestrator peut être différent et est spécifique au fournisseur.

- 2 Pour cet exemple, exécutez le workflow d'enregistrement **Register IPAM Endpoint** et spécifiez le type de point de terminaison IPAM **Infoblox**.
- 3 Lorsque vous êtes invité à saisir les informations d'identification dans vRealize Automation, saisissez vos informations d'identification d'administrateur de vRealize Automation vRA.

Le module enregistre Infoblox comme nouveau type de point de terminaison IPAM dans le service des points de terminaison vRealize Automation et met le type de point de terminaison à disposition lorsque vous définissez les points de terminaison dans vRealize Automation.

Remarque La connexion IPAM Infoblox peut disparaître de l'onglet vRealize Orchestrator **Inventaire** après le redémarrage du serveur vRealize Orchestrator dans le centre de contrôle de vRealize Orchestrator. Pour résoudre ce problème, exécutez le workflow **Create IPAM Connection** à partir de la séquence de menus **vRO admin > Bibliothèque > Infoblox > vRA > Assistance**. Dans l'onglet vRealize Orchestrator **Inventaire**, sélectionnez **IPAM Infoblox** et actualisez la page pour afficher la connexion IPAM Infoblox.

Suivant

Vous pouvez à présent configurer un point de terminaison du type IPAM Infoblox ou un point de terminaison pour n'importe quel module ou plug-in tiers que vous venez d'enregistrer dans vRealize Automation. Reportez-vous à [Créer un point de terminaison de fournisseur IPAM tiers](#).

Liste de contrôle pour configurer Conteneurs pour vRealize Automation

Pour prendre en main Conteneurs, vous devez configurer la fonctionnalité de prise en charge des rôles utilisateur de vRealize Automation.

Après avoir configuré les définitions de conteneur dans Conteneurs, vous pouvez ajouter et configurer des composants de conteneur dans un Blueprint.

Tableau 1-4. Liste de contrôle pour configurer Conteneurs pour vRealize Automation

Tâche	Détails
Affectez les rôles d'administrateur et d'architecte de conteneur.	Reportez-vous aux informations sur les rôles relatifs aux conteneurs de la section <i>Fondements et concepts</i>
Affichez le système d'aide contextuelle de Conteneurs.	Reportez-vous à l'aide sur les rôles relatifs aux conteneurs dans <i>Fondements et concepts</i>
Définissez les conteneurs dans l'onglet Conteneurs dans vRealize Automation.	Reportez-vous à <i>Configuration de vRealize Automation</i> .
Ajoutez des composants de conteneur et des composants réseau de conteneur aux Blueprints dans l'onglet Concevoir de vRealize Automation.	Reportez-vous à <i>Configuration de vRealize Automation</i> .

Configuration de Conteneurs à l'aide du dispositif vRealize Automation

Les informations sur le service Xenon sont accessibles dans le dispositif vRealize Automation vRealize Automation (**Paramètres vRA > Xenon**).

Cette section contient des informations sur la machine virtuelle de l'hôte Xenon, le port d'écoute et l'état du service. Elle présente également des informations sur les nœuds Xenon en cluster.

Vous pouvez gérer le service Linux Xenon depuis l'interface de ligne de commande du dispositif vRealize Automation.

Command	Description
<code>service xenon-service status</code>	Indique si le service est en cours d'exécution ou arrêté.
<code>service xenon-service start</code>	Démarre le service.
<code>service xenon-service stop</code>	Arrête le service.
<code>service xenon-service restart</code>	Redémarre le service.
<code>service xenon-service get_host</code>	Affiche le nom d'hôte sur lequel le service s'exécute.
<code>service xenon-service get_port</code>	Affiche le port du service.
<code>service xenon-service status_cluster</code>	Affiche des informations sur l'ensemble des nœuds en cluster au format JSON.
<code>service xenon-service reset</code>	Supprime le répertoire où Xenon conserve tous les fichiers de configuration et redémarre le service.

Mise en cluster de conteneurs

Vous pouvez utiliser le service Xenon en conjonction avec Conteneurs pour vRealize Automation pour joindre des nœuds à un cluster. Si les nœuds sont en cluster, le service Xenon connecte automatiquement d'autres nœuds lors de son démarrage.

Vous pouvez suivre l'état du cluster dans l'onglet **Xenon** du dispositif vRealize Automation ou en exécutant la commande suivante dans une interface de ligne de commande :

```
service xenon-service status_cluster
```

Xenon fonctionne sur des cluster basés sur des quorums. Le quorum est calculé en utilisant la formule $(\text{number of nodes} / 2) + 1$.

Préparation de votre environnement vCloud Director pour vRealize Automation

Avant de pouvoir intégrer vCloud Director à vRealize Automation, vous devez installer et configurer votre instance de vCloud Director, configurer vos ressources de cloud vSphere et vous identifier ou créer des informations d'identification appropriées pour fournir à vRealize Automation l'accès à votre environnement vCloud Director.

Configurer votre environnement

Configurez vos ressources vSphere et vos ressources de cloud, y compris les centres de données virtuels et les réseaux. Pour plus d'informations, reportez-vous à la documentation vCloud Director.

Informations d'identification requises pour l'intégration

Identifiez-vous ou créez les informations d'identification de l'administrateur de l'organisation ou de l'administrateur système que peuvent utiliser vos administrateurs IaaS vRealize Automation pour que votre environnement vCloud Director soit géré par vRealize Automation comme un point de terminaison.

Considérations concernant le rôle d'utilisateur

Les rôles d'utilisateur vCloud Director dans une organisation n'ont pas besoin de correspondre aux rôles dans les groupes d'activités vRealize Automation. Si le compte d'utilisateur n'existe pas dans vCloud Director, vCloud Director effectue une recherche dans le LDAP ou Active Directory associé et crée le compte utilisateur si l'utilisateur existe dans le magasin d'identités. S'il ne peut pas créer le compte utilisateur, il journalise un avertissement mais la procédure de provisionnement n'échoue pas. La machine provisionnée est ensuite attribuée au compte utilisé pour configurer le point de terminaison vCloud Director.

Pour plus d'informations sur la gestion d'utilisateurs vCloud Director, reportez-vous à la documentation de vCloud Director.

Préparation de votre environnement vCloud Air pour vRealize Automation

Avant d'intégrer vCloud Air à vRealize Automation, vous devez enregistrer votre compte vCloud Air, configurer votre environnement vCloud Air et vous identifier ou créer des informations d'identification appropriées pour fournir à vRealize Automation l'accès à votre environnement.

Configurer votre environnement

Configurez votre environnement comme décrit dans la documentation de vCloud Air.

Informations d'identification requises pour l'intégration

Identifiez-vous ou créez les informations d'identification de l'administrateur de l'infrastructure virtuelle ou de l'administrateur du compte que peuvent utiliser vos administrateurs IaaS vRealize Automation pour que votre environnement vCloud Air soit géré par vRealize Automation comme un point de terminaison.

Considérations concernant le rôle d'utilisateur

Les rôles d'utilisateur vCloud Air dans une organisation n'ont pas besoin de correspondre aux rôles dans les groupes d'activités vRealize Automation. Pour plus d'informations sur la gestion d'utilisateurs vCloud Air, reportez-vous à la documentation de vCloud Air.

Préparation de votre environnement Amazon AWS

Préparez des éléments et des rôles utilisateur dans votre environnement Amazon AWS, préparez Amazon AWS à communiquer avec l'agent invité et l'agent de démarrage de Logiciel et comprenez comment les fonctionnalités Amazon AWS sont mappées aux fonctionnalités vRealize Automation.

Rôles d'utilisateur et informations d'identification Amazon AWS requis pour vRealize Automation

Vous devez configurer des informations d'identification dans Amazon AWS avec les autorisations requises pour permettre à vRealize Automation de gérer votre environnement.

vRealize Automation nécessite des clés d'accès pour les informations d'identification de point de terminaison et ne prend pas en charge les noms et mots de passe d'utilisateur.

■ Rôle et autorisation dans Amazon Web Services

Bien que le rôle d'utilisateur avancé dans AWS fournit à un utilisateur ou à un groupe du service d'annuaire AWS un accès complet aux services et ressources AWS, cela n'est pas obligatoire. Les rôles d'utilisateur disposant de privilèges inférieurs sont également pris en charge. La stratégie de sécurité AWS qui répond aux besoins de la fonctionnalité vRealize Automation est :

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeImages",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeVpcs",
      "ec2:DescribeSubnets",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeVolumes",

      "ec2:DescribeVpcAttribute",
      "ec2:DescribeAddresses",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeImageAttribute",
      "ec2:DescribeInstanceAttribute",
      "ec2:DescribeVolumeStatus",
      "ec2:DescribeVpnConnections",
      "ec2:DescribeRegions",
      "ec2:DescribeTags",
      "ec2:DescribeVolumeAttribute",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeNetworkInterfaceAttribute",

      "ec2:DisassociateAddress",
      "ec2:GetPasswordData",

      "ec2:ImportKeyPair",
      "ec2:ImportVolume",

      "ec2:CreateVolume",
      "ec2>DeleteVolume",
      "ec2:AttachVolume",
      "ec2:ModifyVolumeAttribute",
      "ec2:DetachVolume",

      "ec2:AssignPrivateIpAddresses",
      "ec2:UnassignPrivateIpAddresses",

      "ec2:CreateKeyPair",
      "ec2>DeleteKeyPair",
```

```

        "ec2:CreateTags",
        "ec2:AssociateAddress",
        "ec2:ReportInstanceState",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:MonitorInstances",
        "ec2:RebootInstances",
        "ec2:RunInstances",
        "ec2:TerminateInstances",

        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeInstanceHealth"
    ],
    "Resource": "*"
}
}}
```

■ Informations d'identification d'authentification dans Amazon Web Services

Pour pouvoir gérer les utilisateurs et les groupes IAM (Amazon Identity and Access Management), votre configuration doit inclure des informations d'identification d'administrateur donnant un accès complet à AWS.

Lorsque vous créez un point de terminaison AWS dans vRA, vous êtes invité à entrer une clé et une clé secrète. Pour obtenir la clé d'accès nécessaire pour créer le point de terminaison Amazon, l'utilisateur avancé doit soit demander une clé à un utilisateur disposant d'informations d'identification d'administrateur ayant un accès complet à AWS, soit être également configuré avec la stratégie d'administrateur avec accès complet à AWS. Reportez-vous à [Créer un point de terminaison Amazon](#).

Pour plus d'informations sur l'activation des stratégies et des rôles, reportez-vous à la section *AWS Identity and Access Management (IAM)* de la documentation du produit Amazon Web Services.

Autoriser Amazon AWS à communiquer avec l'agent de démarrage Logiciel et l'agent invité

Si vous prévoyez de provisionner des Blueprints d'application qui contiennent Logiciel ou si vous voulez pouvoir personnaliser davantage des machines provisionnées à l'aide de l'agent invité, activez la connectivité entre l'environnement Amazon AWS, dans lequel les machines sont provisionnées, et l'environnement vRealize Automation, dans lequel les agents téléchargent des modules et reçoivent des instructions.

Lorsque vous utilisez vRealize Automation pour provisionner des machines Amazon AWS avec l'agent invité vRealize Automation et l'agent de démarrage Logiciel, vous devez configurer la connectivité entre le réseau et Amazon VPC (Virtual Private Cloud) afin que les machines provisionnées puissent communiquer avec vRealize Automation pour personnaliser vos machines.

Pour plus d'informations sur les options de connectivité VPC Amazon AWS, reportez-vous à la documentation Amazon AWS.

Utilisation de fonctionnalités Amazon facultatives

vRealize Automation prend en charge plusieurs fonctionnalités Amazon, parmi lesquelles Amazon Virtual Private Cloud, les équilibres de charge élastiques, les adresses IP élastiques et le stockage Elastic Block.

Utilisation des groupes de sécurité Amazon

Spécifiez au moins un groupe de sécurité au moment de la création d'une réservation Amazon. Chaque région disponible nécessite au moins un groupe de sécurité spécifié.

Un groupe de sécurité agit comme un pare-feu afin de contrôler l'accès à une machine. Chaque région inclut au moins le groupe de sécurité par défaut. Les administrateurs peuvent utiliser Amazon Web Services Management Console pour créer des groupes de sécurité supplémentaires, configurer des ports pour Microsoft Remote Desktop Protocol ou SSH et configurer un réseau privé virtuel pour un Amazon VPN.

Lorsque vous créez une réservation Amazon ou que vous configurez un composant de machine dans le Blueprint, vous pouvez choisir parmi la liste des groupes de sécurité disponibles pour la région du compte Amazon spécifié. Les groupes de sécurité sont importés au moment de la collecte de données.

Pour plus d'informations sur la création et l'utilisation de groupes de sécurité dans Amazon Web Services, reportez-vous à la documentation Amazon.

Présentation des régions Amazon Web Service

Chaque compte Amazon Web Services est représenté par un point de terminaison cloud. Lorsque vous créez un point de terminaison Amazon Elastic Cloud Computing dans vRealize Automation, les régions sont recueillies comme des ressources de calcul. Une fois que l'administrateur IaaS a sélectionné des ressources de calcul pour un groupe d'activité, les collectes de données d'inventaire et d'état s'exécutent automatiquement.

La collecte des données d'inventaire, qui s'exécute automatiquement une fois par jour, recueille les données sur la nature d'une ressource de calcul, par exemple :

- adresses IP élastiques,
- équilibres de charge élastiques,
- volumes de stockage des blocs élastiques.

La collecte des données d'état s'exécute automatiquement toutes les 15 minutes par défaut. Elle regroupe les informations concernant l'état des instances gérées, qui sont des instances créées par vRealize Automation. Les éléments suivants sont des exemples de données d'état :

- mots de passe Windows,
- état des machines des équilibres de charge,
- adresses IP élastiques.

Un administrateur Fabric peut lancer une collecte de données d'inventaire et d'état, ainsi que désactiver ou modifier la fréquence de la collecte des données d'état et d'inventaire.

Utilisation d'un cloud privé virtuel (VPC) Amazon

Amazon Virtual Private Cloud vous permet de provisionner des instances de machine Amazon dans une section privée du cloud Amazon Web Services.

Les utilisateurs d'Amazon Web Services peuvent utiliser Amazon VPC pour concevoir une topologie de réseau virtuel en fonction de leurs spécifications. Vous pouvez attribuer un cloud privé virtuel Amazon VPC à vRealize Automation. Néanmoins, vRealize Automation n'effectue pas le suivi du coût de l'utilisation du cloud privé virtuel Amazon VPC.

Lorsque vous effectuez un provisionnement à l'aide du cloud privé virtuel Amazon VPC, vRealize Automation escompte la présence d'un sous-réseau de cloud privé virtuel auprès duquel Amazon obtient une adresse IP principale. Cette adresse est statique jusqu'à ce que l'instance soit arrêtée. Vous pouvez également utiliser le pool d'adresses IP élastiques pour associer également une adresse IP élastique à une instance de vRealize Automation. Cela permet à l'utilisateur de conserver la même adresse IP s'il provisionne et démonte continuellement une instance dans Amazon Web Services.

Utilisez la console AWS Management Console pour créer les éléments suivants :

- Un cloud privé virtuel Amazon VPC qui inclut des passerelles Internet, une table de routage, des groupes de sécurité et des sous-réseaux et des adresses IP disponibles.
- Un réseau Amazon Virtual Private Network si les utilisateurs ont besoin de se connecter aux instances des machines Amazon en dehors de la console AWS Management Console.

Les utilisateurs de vRealize Automation peuvent effectuer les tâches suivantes lorsqu'ils travaillent avec un cloud privé virtuel Amazon VPC :

- Un administrateur Fabric peut attribuer un cloud privé virtuel Amazon VPC à une réservation de cloud. Reportez-vous à [Créer une réservation Amazon EC2](#).
- Un propriétaire de machine peut attribuer une instance de machine Amazon à un cloud privé virtuel Amazon VPC.

Pour plus d'informations sur la création d'un cloud privé virtuel Amazon VPC, reportez-vous à la documentation Amazon Web Services.

Utilisation d'équilibrages de charge élastiques pour Amazon Web Services

Les équilibrages de charge élastiques distribuent le trafic d'application entrant dans les instances de Amazon Web Services. L'équilibrage de charge Amazon permet d'améliorer la tolérance aux pannes et les performances.

Amazon met à disposition l'équilibrage de charge élastique pour les machines provisionnées à l'aide de Blueprints Amazon EC2.

L'équilibrage de charge élastique doit être disponible dans Amazon Web Services, Amazon Virtual Private Network et à l'emplacement du provisionnement. Par exemple, si un équilibrage de charge est disponible dans us-east1c et que la machine se situe dans us-east1b, la machine ne peut pas utiliser l'équilibrage de charge disponible.

vRealize Automation ne permet pas de créer, gérer ou surveiller les équilibrages de charge élastiques.

Pour plus d'informations sur la création d'équilibrages de charge élastiques Amazon à l'aide de Amazon Web Services Management Console, reportez-vous à la documentation Amazon Web Services.

Utilisation d'adresses IP élastiques pour Amazon Web Services

L'utilisation d'une adresse IP élastique vous permet de basculer rapidement vers une autre machine dans un environnement de cloud Amazon Web Services dynamique. Dans vRealize Automation, l'adresse IP élastique est disponible pour tous les groupes d'activité disposant de droits sur la région.

Un administrateur peut allouer des adresses IP élastiques à votre compte Amazon Web Services à l'aide de la AWS Management Console. Il existe deux groupes d'adresses IP élastiques dans les régions : un groupe est alloué aux instances autres que Amazon VPC et l'autre groupe est alloué à Amazon VPC. Si vous allouez des adresses dans une région autre que Amazon VPC uniquement, ces adresses ne sont disponibles dans aucune instance d'Amazon VPC. Le contraire est également vrai. Si vous allouez des adresses dans un Amazon VPC uniquement, celles-ci ne sont pas disponibles dans une région autre que Amazon VPC.

L'adresse IP élastique est associée au compte Amazon Web Services. Même si elle n'est associée à aucune machine particulière, une seule machine à la fois peut utiliser cette adresse. L'adresse reste associée à votre compte Amazon Web Services jusqu'à ce que vous décidiez de la remettre à disposition. Vous pouvez faire cela pour la mapper à une instance de machine spécifique.

Un architecte IaaS peut ajouter une propriété personnalisée à un Blueprint afin d'attribuer une adresse IP élastique à des machines lors du provisionnement. Les propriétaires et les administrateurs de machines peuvent afficher les adresses IP élastiques attribuées aux machines. Les propriétaires ou les administrateurs de machines disposant du droit de modifier les machines peuvent attribuer une adresse IP élastique après le provisionnement. Néanmoins, si l'adresse est déjà associée à une instance de machine et que celle-ci fait partie du déploiement Amazon Virtual Private Cloud, Amazon n'attribue pas l'adresse.

Pour plus d'informations sur la création et l'utilisation d'adresses IP élastiques Amazon, reportez-vous à la documentation Amazon Web Services.

Utilisation du stockage Elastic Block pour Amazon Web Services

Le stockage Amazon Elastic Block fournit des volumes de stockage au niveau des blocs à utiliser avec une instance de machine Amazon et Amazon Virtual Private Cloud. Le volume de stockage peut persister au-delà de la durée de vie de son instance de machine Amazon associée dans l'environnement de cloud Amazon Web Services.

Lorsque vous utilisez un volume de stockage Amazon Elastic Block conjointement à vRealize Automation, tenez compte des mises en garde suivantes :

- Vous ne pouvez pas associer un volume de stockage Elastic Block existant lorsque vous provisionnez une instance de machine. En revanche, si vous créez un nouveau volume et que vous demandez plusieurs machines à la fois, le volume est créé et associé à chaque instance. Par exemple, si vous créez un volume nommé volume_1 et que vous demandez trois machines, un volume est créé pour chaque machine. Trois volumes nommés volume_1 sont créés et associés à chaque machine. Chaque volume a un ID de volume unique. Chaque volume possède la même taille et le même emplacement.

- Le volume doit avoir le même système d'exploitation et se trouver au même emplacement que la machine à laquelle vous l'associez.
- vRealize Automation ne gère pas le volume principal d'une instance sauvegardée sur un stockage Elastic Block.

Pour plus d'informations sur le stockage Amazon Elastic Block et pour obtenir des détails sur son activation à l'aide de la Amazon Web Services Management Console, reportez-vous à la documentation Amazon Web Services.

Scénario : configurer la connectivité VPC entre le réseau et Amazon pour un environnement de validation technique

En tant que professionnel informatique configurant un environnement de validation technique afin d'évaluer vRealize Automation, vous souhaitez configurer de façon temporaire une connectivité entre le réseau et Amazon VPC, afin de prendre en charge la fonctionnalité vRealize Automation Logiciel.

La connectivité entre le réseau et Amazon VPC n'est obligatoire que si vous souhaitez utiliser l'agent invité pour personnaliser les machines provisionnées, ou si vous souhaitez inclure à des Blueprints des composants Logiciel. Dans un environnement de production, vous configurerez cette connectivité de façon officielle par le biais de Amazon Web Services. Cependant, puisque vous travaillez dans un environnement de validation technique, vous souhaitez configurer une connectivité temporaire entre le réseau et Amazon VPC. Vous établissez le tunnel SSH, puis configurez une réservation Amazon dans vRealize Automation pour l'acheminement via votre tunnel.

Prérequis

- Installez et configurez entièrement vRealize Automation. Reportez-vous à *Installation et configuration de vRealize Automation pour le scénario Rainpole*.
- Créez un groupe de sécurité Amazon AWS appelé TunnelGroup et configurez-le de sorte qu'il autorise l'accès au port 22.
- Créez ou identifiez une machine CentOS dans le groupe de sécurité TunnelGroup Amazon AWS et notez les configurations suivantes :
 - Informations d'identification de l'utilisateur administratif, par exemple *racine*
 - Adresse IP publique
 - Adresse IP privée
- Créez ou identifiez une machine CentOS sur le même réseau local que l'installation de vRealize Automation.
- Installez le serveur SSHD OpenSSH sur les deux machines tunnel.

Procédure

- 1 Connectez-vous à la machine tunnel Amazon AWS en tant qu'utilisateur racine ou un rôle similaire.

2 Désactivez les tables d'IP.

```
# service iptables save
# service iptables stop
# chkconfig iptables off
```

3 Modifiez /etc/ssh/sshd_config pour activer AllowTCPForwarding et GatewayPorts.

4 Redémarrez le service.

```
/etc/init.d/sshd restart
```

5 Connectez-vous à la machine CentOS en tant qu'utilisateur racine sur le même réseau local que l'installation vRealize Automation.

6 Appelez le tunnel SSH à partir de la machine du réseau local vers la machine tunnel Amazon AWS.

```
ssh -N -v -o "ServerAliveInterval 30" -o "ServerAliveCountMax 40" -o "TCPKeepAlive yes" \

-R 1442:vRealize_automation_appliance_fqdn:5480 \
-R 1443:vRealize_automation_appliance_fqdn:443 \
-R 1444:manager_service_fqdn:443 \
Utilisateur de la machine tunnel Amazon@Adresse IP publique de la machine tunnel Amazon
```

Vous configurez un réacheminement de port pour permettre à votre machine du tunnel Amazon AWS d'accéder aux ressources vRealize Automation, mais votre tunnel SSH ne fonctionne pas tant que vous n'avez pas configuré une réservation Amazon pour l'acheminement via le tunnel.

Suivant

- 1 Installez l'agent de démarrage logiciel et l'agent invité sur une machine de référence Windows ou Linux, afin de créer une image de machine Amazon que les architectes IaaS peuvent utiliser pour créer des Blueprints. Reportez-vous à [Préparation du provisionnement Logiciel](#).
- 2 Configurez votre réservation Amazon dans vRealize Automation pour l'acheminement via votre tunnel SSH. Reportez-vous à [Scénario : créer une réservation Amazon pour un environnement de validation technique](#).

Préparation des fonctionnalités Réseau et sécurité de Red Hat OpenStack

vRealize Automation prend en charge plusieurs fonctionnalités dans OpenStack, notamment les groupes de sécurité et les adresses IP flottantes. Apprenez comment fonctionnent ces fonctionnalités avec vRealize Automation et configurez-les dans votre environnement.

Utilisation des groupes de sécurité OpenStack

Les groupes de sécurité vous permettent de spécifier des règles permettant de contrôler le trafic réseau sur des ports spécifiques.

Vous pouvez spécifier des groupes de sécurité dans une réservation lorsque vous demandez une machine. Vous pouvez également spécifier un groupe de sécurité NSX existant ou à la demande dans le canevas de conception.

Les groupes de sécurité sont importés au moment de la collecte de données.

Chaque région disponible nécessite au moins un groupe de sécurité spécifié. Lorsque vous créez une réservation, les groupes de sécurité disponibles pour vous dans cette région sont affichés. Chaque région inclut au moins le groupe de sécurité par défaut.

Les groupes de sécurité supplémentaires doivent être gérés dans la ressource source. Pour plus d'informations sur la gestion des groupes de sécurité des différentes machines, reportez-vous à la documentation d'OpenStack.

Utilisation d'adresses IP flottantes avec OpenStack

Vous pouvez attribuer des adresses IP flottantes à une instance virtuelle en cours d'exécution dans OpenStack

Pour permettre l'attribution d'adresses IP flottantes, vous devez configurer la transmission d'adresses IP et créer un pool d'adresses IP dans Red Hat OpenStack. Pour plus d'informations, consultez la documentation Red Hat OpenStack.

Vous devez autoriser les actions Associer une adresse IP flottante et Dissocier les adresses IP flottantes aux propriétaires des machines. Les utilisateurs autorisés peuvent alors associer une adresse IP flottante à une machine provisionnée à partir des réseaux externes associés à la machine en sélectionnant une adresse disponible dans le pool d'adresses IP flottantes. Lorsqu'une adresse IP flottante a été associée à une machine, un utilisateur de vRealize Automation peut sélectionner une option Dissocier les adresses IP flottantes pour afficher les adresses IP flottantes attribuées actuellement et dissocier une adresse d'une machine.

Préparation de votre environnement SCVMM

Avant de commencer à créer des modèles de SCVMM et des profils matériels à utiliser lors du provisionnement de machines vRealize Automation, vous devez comprendre les restrictions concernant la dénomination de modèles et de profils matériels et configurer les paramètres réseau et de stockage de SCVMM.

Pour des informations complémentaires sur la préparation de votre environnement, reportez-vous à la rubrique Exigences SCVMM dans *Installation de vRealize Automation 7.3*.

Pour des informations complémentaires sur le provisionnement de machine, reportez-vous à [Créer un point de terminaison Hyper-V \(SCVMM\)](#).

vRealize Automation ne prend pas en charge un environnement de déploiement qui utilise une configuration de cloud privé SCVMM. Actuellement, vRealize Automation ne peut pas effectuer de collecte dans des clouds privés SCVMM, faire des allocations à ces clouds ni effectuer de provisionnement basé sur ces clouds

Dénomination de modèles et de profils matériels

Du fait des conventions de dénomination utilisées par SCVMM et vRealize Automation pour les modèles et les profils matériels, ne faites pas commencer les noms de vos modèles ou de vos profils matériels par les mots « temporary » ou « profile ». Par exemple, les termes suivants sont ignorés au cours de la collecte de données :

- TemporaryTemplate
- Temporary Template
- TemporaryProfile
- Temporary Profile
- Profile

Configuration réseau requise pour les clusters SCVMM

Les clusters SCVMM exposent uniquement des réseaux virtuels à vRealize Automation. Vous devez donc avoir une relation bilatérale entre votre réseau virtuel et votre réseau logique. À l'aide la console SCVMM, mappez chaque réseau logique à un réseau virtuel et configurez votre cluster SCVMM pour qu'il accède aux machines à l'aide du réseau virtuel.

Configuration de stockage requise pour les clusters SCVMM

Sur des clusters Hyper-V SCVMM, vRealize Automation collecte des données et effectue des provisionnements uniquement sur des volumes partagés. À l'aide de la console SCVMM, configurez vos clusters afin d'utiliser des volumes de ressources partagés pour le stockage.

Configuration de stockage requise pour les hôtes SCVMM autonomes

Pour les hôtes SCVMM autonomes, vRealize Automation collecte des données et effectue des provisionnements sur le chemin d'accès à une machine virtuelle par défaut. À l'aide de la console SCVMM, configurez des chemins d'accès à une machine virtuelle par défaut pour vos hôtes autonomes.

Configurer la connectivité VPC entre le réseau et Azure

Vous devez configurer la connectivité entre le réseau et Azure si vous souhaitez utiliser des composants logiciels dans des blueprints Azure.

Prérequis

- Installez et configurez entièrement vRealize Automation. Reportez-vous à *Installation et configuration de vRealize Automation pour le scénario Rainpole*.
- Créez un groupe de sécurité Azure appelé TunnelGroup et configurez-le de sorte qu'il autorise l'accès au port 22.

- Créez ou identifiez une machine CentOS dans le groupe de sécurité TunnelGroup Azure et notez les configurations suivantes :
 - Informations d'identification de l'utilisateur administratif, par exemple *racine*
 - Adresse IP publique
 - Adresse IP privée
- Créez ou identifiez une machine CentOS sur le même réseau local que l'installation de vRealize Automation.
- Installez le serveur SSHD OpenSSH sur les deux machines tunnel.

Procédure

- 1 Connectez-vous à la machine tunnel Azure en tant qu'utilisateur racine ou un rôle similaire.
- 2 Désactivez les tables d'IP.

```
# service iptables save
# service iptables stop
# chkconfig iptables off
```

- 3 Modifiez `/etc/ssh/sshd_config` pour activer `AllowTCPForwarding` et `GatewayPorts`.
- 4 Redémarrez le service.

```
/etc/init.d/sshd restart
```

- 5 Connectez-vous à la machine CentOS en tant qu'utilisateur racine sur le même réseau local que l'installation vRealize Automation.
- 6 Appelez le tunnel SSH à partir de la machine du réseau local vers la machine du tunnel Azure.

```
ssh -N -v -o "ServerAliveInterval 30" -o "ServerAliveCountMax 40" -o "TCPKeepAlive yes" \
-R 1442:vRealize_automation_appliance_fqdn:5480 \
-R 1443:vRealize_automation_appliance_fqdn:443 \
-R 1444:manager_service_fqdn:443 \
Utilisateur de la machine tunnel Azure@Adresse IP publique de la machine tunnel Azure
```

Vous avez configuré un réacheminement de port pour permettre à votre machine tunnel Azure d'accéder aux ressources vRealize Automation, mais votre tunnel SSH ne fonctionne pas tant que vous n'avez pas configuré une réservation Amazon pour l'acheminement via le tunnel.

Suivant

- 1 Installez l'agent de démarrage logiciel et l'agent invité sur une machine de référence Windows ou Linux, afin de créer une image de machine Azure que les architectes IaaS peuvent utiliser pour créer des Blueprints. Reportez-vous à [Préparation du provisionnement Logiciel](#).
- 2 Configurez votre réservation Azure dans vRealize Automation pour l'acheminement via votre tunnel SSH. Reportez-vous à [Créer une réservation pour Microsoft Azure](#).

Préparation du provisionnement de machines

En fonction de votre environnement et de votre méthode de provisionnement de machines, vous devrez éventuellement configurer des éléments en dehors de vRealize Automation.

Par exemple, vous devrez éventuellement configurer des modèles de machines ou des images de machines. Vous devrez peut-être également configurer des paramètres NSX ou exécuter des workflows vRealize Orchestrator.

Pour plus d'informations sur la spécification de ports lors de la préparation du provisionnement de machines, reportez-vous à *Guide sur la configuration sécurisée* et à *Architecture de référence* dans la page [Informations sur VMware vRealize Automation](#).

Choix d'une méthode de provisionnement de machine à préparer

Pour la plupart des méthodes de provisionnement de machine, vous devez préparer certains éléments à l'extérieur de vRealize Automation.

Tableau 1-5. Choix d'une méthode de provisionnement de machine à préparer

Scénario	Point de terminaison pris en charge	Prise en charge de l'agent	Méthode de provisionnement	Préparations de pré-provisionnement
Configurez vRealize Automation pour exécuter des scripts Visual Basic personnalisés comme étapes supplémentaires dans le cycle de vie des machines, avant ou après le provisionnement des machines. Par exemple, vous pourriez utiliser un script de pré-provisionnement pour générer les certificats ou les jetons de sécurité avant le provisionnement, puis un script de post-provisionnement pour utiliser les certificats et les jetons après le provisionnement des machines.	Vous pouvez exécuter des scripts Visual Basic avec tous les points de terminaison pris en charge excepté Amazon AWS.	Dépend de la méthode de provisionnement que vous choisissez.	Pris en charge en tant qu'étape supplémentaire de n'importe quelle méthode de provisionnement, mais vous ne pouvez pas utiliser des scripts Visual Basic avec des machines Amazon AWS.	Liste de contrôle pour l'exécution de scripts Visual Basic lors du provisionnement
Provisionnez des Blueprints d'application qui automatisent l'installation, la configuration et la gestion du cycle de vie des composants des déploiements d'intergiciels et d'applications comme Oracle, MySQL, WAR et les schémas de base de données.	<ul style="list-style-type: none"> ■ vSphere ■ vCloud Air ■ vCloud Director ■ Amazon AWS 	<ul style="list-style-type: none"> ■ (Obligatoire) Agent invité ■ (Obligatoire) Agent de démarrage logiciel et agent invité 	<ul style="list-style-type: none"> ■ Cloner ■ Cloner (pour vCloud Air ou vCloud Director) ■ Clone lié ■ Image de la machine Amazon 	Si vous souhaitez pouvoir utiliser les composants des Logiciel dans vos Blueprints, préparez une méthode de provisionnement qui prenne en charge l'agent invité et l'agent de démarrage des Logiciel. Pour plus d'informations sur la préparation des Logiciel, reportez-vous à Préparation du provisionnement Logiciel .
Personnalisez davantage les machines à l'issue du provisionnement à l'aide de l'agent invité.	Tous les points de terminaison virtuels et Amazon AWS.	<ul style="list-style-type: none"> ■ (Obligatoire) Agent invité ■ (Facultatif) Agent de démarrage logiciel et agent invité 	Pris en charge pour toutes les méthodes de provisionnement excepté l'image de machine virtuelle.	Si vous souhaitez pouvoir personnaliser des machines à l'issue du provisionnement, sélectionnez une méthode de provisionnement qui prenne en charge l'agent invité. Pour plus d'informations sur l'agent invité, reportez-vous à Utilisation d'un agent invité vRealize Automation dans un provisionnement .

Tableau 1-5. Choix d'une méthode de provisionnement de machine à préparer (suite)

Scénario	Point de terminaison pris en charge	Prise en charge de l'agent	Méthode de provisionnement	Préparations de pré-provisionnement
Provisionnez des machines sans système d'exploitation invité. Vous pouvez installer un système d'exploitation après le provisionnement.	Tous les points de terminaison de machines virtuelles.	Non pris en charge.	De base	Aucune préparation de pré-provisionnement requise à l'extérieur de vRealize Automation.
Provisionnez une copie de machine virtuelle disposant d'un espace suffisant appelée clone lié. Les clones liés sont basés sur un snapshot de machine virtuelle et utilisent une chaîne de disques delta pour effectuer le suivi des différences avec la machine parent.	vSphere	<ul style="list-style-type: none"> ■ (Facultatif) Agent invité ■ (Facultatif) Agent de démarrage logiciel et agent invité 	Clone lié	<p>Vous devez disposer d'une machine virtuelle vSphere existante.</p> <p>Si vous souhaitez prendre en charge Logiciel, vous devez installer l'agent invité et l'agent de démarrage logiciel sur la machine que vous souhaitez cloner.</p> <p>Le snapshot de machine virtuelle identifié dans le Blueprint doit être désactivé avant de provisionner les machines virtuelles de clones liés.</p>
Provisionnez une copie de machine virtuelle disposant d'un espace suffisant à l'aide de la technologie Net App FlexClone.	vSphere	(Facultatif) Agent invité	NetApp FlexClone	Liste de vérification pour la préparation du provisionnement par le clonage
Provisionnez des machines en clonant un modèle d'objet créer à partir d'une machine Windows ou Linux existante, appelée la machine de référence et un objet de personnalisation.	<ul style="list-style-type: none"> ■ vSphere ■ KVM (RHEV) ■ SCVMM 	<ul style="list-style-type: none"> ■ (Facultatif) Agent invité ■ (Facultatif pour vSphere uniquement) Agent de démarrage logiciel et agent invité 	Cloner	<p>Reportez-vous à Liste de vérification pour la préparation du provisionnement par le clonage.</p> <p>Si vous souhaitez prendre en charge Logiciel, vous devez installer l'agent invité et l'agent de démarrage logiciel sur la machine vSphere que vous souhaitez cloner.</p>
Provisionnez des machines vCloud Air ou vCloud Director en clonant à partir d'un modèle et d'un objet de personnalisation.	<ul style="list-style-type: none"> ■ vCloud Air ■ vCloud Director 	<ul style="list-style-type: none"> ■ (Facultatif) Agent invité ■ (Facultatif) Agent de démarrage logiciel et agent invité 	Clonage de vCloud Air ou vCloud Director	<p>Reportez-vous à Préparation pour le provisionnement vCloud Air et vCloud Director.</p> <p>Si vous souhaitez prendre en charge Logiciel, créez un modèle qui contienne l'agent invité et l'agent de démarrage logiciel. Pour vCloud Air, configurez la connectivité réseau entre votre environnement vRealize Automation et votre environnement vCloud Air.</p>

Tableau 1-5. Choix d'une méthode de provisionnement de machine à préparer (suite)

Scénario	Point de terminaison pris en charge	Prise en charge de l'agent	Méthode de provisionnement	Préparations de pré-provisionnement
Provisionnez une machine en effectuant un démarrage à partir d'une image ISO, à l'aide d'un fichier de configuration kickstart ou autoYaSt et une image de distribution Linux pour installer le système d'exploitation sur la machine.	<ul style="list-style-type: none"> Tous les points de terminaison virtuels. Red Hat OpenStack 	L'agent invité est installé conformément aux instructions de préparation.	Kickstart Linux	Préparation du provisionnement Kickstart Linux
Provisionnez une machine et transmettez le contrôle à une séquence de tâches SCCM pour effectuer un démarrage à partir d'une image ISO, déployer un système d'exploitation Windows et installez l'agent invité vRealize Automation.	Tous les points de terminaison de machines virtuelles.	L'agent invité est installé conformément aux instructions de préparation.	SCCM	Préparation du provisionnement SCCM
Provisionnez une machine en effectuant un démarrage dans un environnement WinPE et en installant un système d'exploitation à l'aide de l'image au format WIM d'une machine de référence Windows.	<ul style="list-style-type: none"> Tous les points de terminaison virtuels. Red Hat OpenStack 	L'agent invité est obligatoire. Lorsque vous créez l'image WinPE, vous devez insérer manuellement l'agent invité.	WIM	Préparation du provisionnement de WIM
Lancez une instance depuis une image de machine virtuelle.	Red Hat OpenStack	Non pris en charge.	Image de machine virtuelle	Reportez-vous à Préparation du provisionnement de l'image de machine virtuelle .
Lancez une instance depuis une image de la machine Amazon.	Amazon AWS	<ul style="list-style-type: none"> (Facultatif) Agent invité (Facultatif) Agent de démarrage logiciel et agent invité 	Image de la machine Amazon	<p>Associez les images des machines Amazon et les types d'instances à votre compte Amazon AWS.</p> <p>Si vous souhaitez prendre en charge Logiciel, créez une image de machine Amazon qui contienne l'agent invité et l'agent de démarrage logiciel, puis configurez la connectivité réseau-VPC entre vos environnements Amazon AWS et vRealize Automation.</p>

Liste de contrôle pour l'exécution de scripts Visual Basic lors du provisionnement

Vous pouvez configurer vRealize Automation pour exécuter vos scripts Visual Basic personnalisés comme étapes supplémentaires dans le cycle de vie des machines, avant ou après le provisionnement des machines. Par exemple, vous pourriez utiliser un script de pré-provisionnement pour générer les certificats ou les jetons de sécurité avant le provisionnement, puis un script de post-provisionnement pour utiliser les certificats et les jetons après le provisionnement des machines. Vous pouvez exécuter des scripts Visual Basic avec n'importe quelle méthode de provisionnement, mais vous ne pouvez pas utiliser des scripts Visual Basic avec des machines Amazon AWS.

Tableau 1-6. Liste de contrôle pour l'exécution de scripts Visual Basic lors du provisionnement

Tâche	Emplacement	Détails
<input type="checkbox"/> Installez et configurez l'agent EPI pour les scripts Visual Basic.	Généralement l'hôte Manager Service	Reportez-vous à <i>Installation de vRealize Automation 7.3</i> .
<input type="checkbox"/> Créez vos scripts Visual Basic.	Machine sur laquelle l'agent EPI est installé	<p>vRealize Automation inclut un modèle de script Visual Basic <code>PrePostProvisioningExample.vbs</code> dans le sous-répertoire <code>Scripts</code> du répertoire d'installation de l'agent EPI. Ce script contient un en-tête pour charger tous les arguments dans un dictionnaire, un corps de texte dans lequel vous pouvez inclure vos fonctions, et un pied de page pour renvoyer les propriétés personnalisées mises à jour à vRealize Automation.</p> <p>Lors de l'exécution d'un script Visual Basic, l'agent EPI transmet toutes les propriétés personnalisées des machines comme arguments au script. Pour renvoyer les valeurs des propriétés mises à jour à vRealize Automation, placez ces propriétés dans un dictionnaire et appelez une fonction fournie par vRealize Automation.</p>
<input type="checkbox"/> Recueillez les informations requises pour inclure vos scripts dans des Blueprints.	<p>Capturez les informations et transférez-les à vos architectes d'infrastructure</p> <p>Remarque Un administrateur Fabric peut créer un groupe de propriétés en utilisant les jeux de propriétés <code>ExternalPreProvisioningVbScript</code> et <code>ExternalPostProvisioningVbScript</code> pour fournir les informations requises. Cela permet aux architectes du Blueprint d'inclure facilement et correctement ces informations à leurs Blueprints.</p>	<ul style="list-style-type: none"> ■ Chemin complet du script Visual Basic, y compris le nom du fichier et l'extension. Par exemple, <code>%System Drive%Program Files (x86)\VMware\VCAC Agents\EPI_Agents\Scripts\SendEmail.vbs</code>. ■ Pour exécuter un script avant le provisionnement, demandez aux architectes d'infrastructure d'entrer le chemin d'accès complet au script comme valeur de la propriété personnalisée <code>ExternalPreProvisioningVbScript</code>. Pour exécuter un script après le provisionnement, ils doivent utiliser la propriété personnalisée <code>ExternalPostProvisioningVbScript</code>.

Utilisation d'un agent invité vRealize Automation dans un provisionnement

Vous pouvez installer l'agent invité sur des machines de référence afin de personnaliser davantage une machine après le déploiement. Vous pouvez utiliser les propriétés personnalisées de l'agent invité réservé pour effectuer des personnalisations de base, comme l'ajout ou le formatage de disques. Vous pouvez également créer vos propres scripts personnalisés pour que l'agent invité s'exécute avec le système d'exploitation invité d'une machine provisionnée.

Une fois le déploiement terminé et la spécification de personnalisation exécutée (si vous en avez fourni une), l'agent invité crée un fichier XML contenant toutes les propriétés personnalisées de la machine déployée, `c:\VRMGuestAgent\site\workitem.xml`, effectue toutes les tâches qui lui sont attribuées avec les propriétés personnalisées de l'agent puis se supprime lui-même de la machine provisionnée.

Vous pouvez écrire vos propres scripts personnalisés pour que l'agent invité s'exécute sur des machines déployées. Vous pouvez également utiliser des propriétés personnalisées sur le Blueprint de la machine pour spécifier l'emplacement de ces scripts et l'ordre dans lequel les exécuter. Vous pouvez également utiliser des propriétés personnalisées sur le Blueprint de la machine pour transmettre des valeurs de propriétés personnalisées à vos scripts en tant que paramètres.

Par exemple, vous pouvez utiliser l'agent invité pour effectuer les personnalisations suivantes sur les machines déployées :

- Changer l'adresse IP
- Ajouter ou formater des disques
- Exécuter des scripts de sécurité
- Initialiser un autre agent, par exemple Puppet ou Chef

Vous pouvez également fournir une chaîne chiffrée en tant que propriété personnalisée dans un argument de ligne de commande. Cela vous permet de stocker des informations chiffrées que l'agent invité peut déchiffrer et comprendre comme un argument de ligne de commande valide.

Remarque L'agent invité Linux attribue des adresses IP statiques lors des actions de création et de clonage pour Linux Kickstart et le provisionnement PXE concernant les propriétés personnalisées de vRealize Automation dans les éléments de travail. L'agent invité ne peut pas prendre en charge le schéma de dénomination réseau cohérente le plus récent, comme dans Ubuntu 16.x, lorsqu'il attribue des adresses IP statiques.

Vos scripts personnalisés n'ont pas besoin d'être installés localement sur la machine. Tant que la machine provisionnée dispose d'un accès réseau à l'emplacement du script, l'agent invité peut accéder aux scripts et les exécuter. Cela diminue les coûts de maintenance, car vous pouvez mettre à jour vos scripts sans avoir à recréer tous vos modèles.

Vous pouvez configurer des paramètres de sécurité pour les machines virtuelles à provisionner en spécifiant des informations dans un script de réservation, de Blueprint ou d'agent invité. Si les machines à provisionner nécessitent un agent invité, vous devez ajouter une règle de sécurité contenant cette exigence à la réservation ou au Blueprint. Par exemple, si vous utilisez une stratégie de sécurité par défaut qui refuse la communication entre toutes les machines, et vous fiez à une stratégie de sécurité distincte qui autorise la communication entre des machines spécifiques, l'agent invité doit être en mesure de communiquer avec vRealize Automation pendant la phase de personnalisation. Pour éviter ce problème lors du provisionnement des machines, utilisez une stratégie de sécurité par défaut qui autorise la communication pendant la phase de personnalisation.

Si vous décidez d'installer l'agent invité pour exécuter des scripts personnalisés sur des machines provisionnées, vos Blueprints doivent inclure les propriétés personnalisées correspondantes de l'agent invité. Par exemple, si vous installez l'agent invité sur un modèle pour du clonage, que vous créez un script personnalisé qui modifie l'adresse IP de la machine provisionnée et que vous placez le script à un emplacement partagé, vous devez inclure un certain nombre de propriétés personnalisées dans votre Blueprint.

Tableau 1-7. Propriétés personnalisées permettant de modifier l'adresse IP d'une machine provisionnée avec un agent invité

Propriété personnalisée	Description
VirtualMachine.Admin.UseGuestAgent	Définissez sur true pour initialiser l'agent invité au démarrage de la machine provisionnée.
VirtualMachine.Customize.WaitComplete	Définissez cette propriété sur True pour empêcher le workflow de provisionnement d'envoyer des éléments de travail à l'agent invité tant que toutes les personnalisations ne sont pas terminées.

Tableau 1-7. Propriétés personnalisées permettant de modifier l'adresse IP d'une machine provisionnée avec un agent invité (suite)

Propriété personnalisée	Description
VirtualMachine.SoftwareN.ScriptPath	<p>Spécifie le chemin d'accès complet à un script d'installation d'application. Le chemin doit être un chemin absolu valide tel qu'il est détecté par le système d'exploitation invité et doit inclure le nom d'un fichier de script.</p> <p>Vous pouvez transmettre les valeurs de propriété personnalisée comme paramètres au script en insérant <code>{CustomPropertyName}</code> dans la chaîne du chemin d'accès. Par exemple, si vous avez une propriété personnalisée appelée <code>ActivationKey</code> dont la valeur est 1234, le chemin d'accès au script est <code>D:\InstallApp.bat -key {ActivationKey}</code>. L'agent invité exécute la commande <code>D:\InstallApp.bat -key 1234</code>. Votre fichier de script peut alors être planifié pour accepter et utiliser cette valeur.</p> <p>Insérez <code>{Owner}</code> pour transmettre le nom du propriétaire de la machine au script.</p> <p>Vous pouvez également transmettre des valeurs de propriétés personnalisées au script sous forme de paramètres en insérant <code>{YourCustomProperty}</code> dans la chaîne du chemin d'accès. Par exemple, si vous entrez la valeur <code>\\vra-scripts.mycompany.com\scripts\changeIP.bat</code>, cela exécute le script <code>changeIP.bat</code> à un emplacement partagé, mais si vous entrez la valeur <code>\\vra-scripts.mycompany.com\scripts\changeIP.bat {VirtualMachine.Network0.Address}</code>, cela exécute le script <code>changeIP</code> et transmet également la valeur de la propriété <code>VirtualMachine.Network0.Address</code> au script sous forme de paramètre.</p>
VirtualMachine.ScriptPath.Decrypt	<p>Permet à vRealize Automation d'obtenir une chaîne chiffrée qui est passée sous la forme d'une instruction de propriété personnalisée <code>VirtualMachine.SoftwareN.ScriptPath</code> correctement formatée à la ligne de commande gupent.</p> <p>Vous pouvez fournir une chaîne chiffrée, par exemple votre mot de passe, en tant que propriété personnalisée dans un argument de ligne de commande. Cela vous permet de stocker des informations chiffrées que l'agent invité peut déchiffrer et interpréter comme un argument de ligne de commande valide. Par exemple, la chaîne de propriété personnalisée <code>VirtualMachine.Software0.ScriptPath = c:\dosomething.bat password</code> n'est pas sécurisée, car elle contient un mot de passe actuel.</p>

Tableau 1-7. Propriétés personnalisées permettant de modifier l'adresse IP d'une machine provisionnée avec un agent invité (suite)

Propriété personnalisée	Description
	<p>Pour chiffrer le mot de passe, vous pouvez créer une propriété personnalisée vRealize Automation, par exemple <code>MyPassword = password</code>, et activer le chiffrement en cochant la case disponible. L'agent invité déchiffre l'entrée <code>[MyPassword]</code> dans la valeur contenue dans la propriété personnalisée <code>MyPassword</code> et exécute le script <code>c:\dosomething.bat password</code>.</p> <ul style="list-style-type: none"> ■ Créez la propriété personnalisée <code>MyPassword = password</code> où <i>password</i> est la valeur de votre mot de passe actuel. Activez le chiffrement en cochant la case disponible. ■ Définissez la propriété personnalisée <code>VirtualMachine.ScriptPath.Decrypt</code> comme <code>VirtualMachine.ScriptPath.Decrypt = true</code>. ■ Définissez la propriété personnalisée <code>VirtualMachine.Software0.ScriptPath</code> comme <code>VirtualMachine.Software0.ScriptPath = c:\dosomething.bat [MyPassword]</code>. <p>Si vous définissez <code>VirtualMachine.ScriptPath.Decrypt</code> sur <code>false</code> ou si vous ne créez pas la propriété personnalisée <code>VirtualMachine.ScriptPath.Decrypt</code>, la chaîne à l'intérieur des crochets ([et]) n'est pas déchiffrée.</p>

Pour plus d'informations sur les propriétés personnalisées que vous pouvez utiliser avec l'agent invité, reportez-vous à la section *Référence des propriétés personnalisées*.

Configurer l'agent invité pour approuver un serveur

L'installation du fichier PEM de clé publique pour l'hôte Manager Service de vRealize Automation dans le dossier correct d'agent invité constitue l'approche la plus sécurisée de configuration de l'agent invité pour approuver un serveur.

Recherchez le dossier d'agent invité dans chaque modèle pour le fichier PEM `cert.pem` de l'hôte Manager Service pour approuver un serveur :

- Dossier d'agent invité Windows de tout modèle utilisant la ligne de commande gagent

```
C:\VRMGuestAgent\cert.pem
```

- Dossier d'agent invité Linux de tout modèle utilisant la ligne de commande gagent

```
/usr/share/gagent/cert.pem
```

Si vous ne placez pas le fichier `cert.pem` à cet emplacement, la machine de référence du modèle ne peut pas utiliser l'agent invité. Par exemple, si vous essayez de collecter les informations de clé publique après le démarrage de la machine virtuelle en modifiant les scripts, vous violez la condition de sécurité.

Des considérations supplémentaires sont à prendre en compte selon l'environnement configuré :

- Pour les installations WIM, vous devez ajouter le contenu du fichier PEM de la clé publique au fichier exécutable de la console et à l'interface utilisateur. L'indicateur de la console est **/cert filename**.
- Pour les installations kickstart de RedHat, vous devez couper/coller la clé publique dans le fichier d'exemple, faute de quoi l'agent invité ne pourra pas s'exécuter.
- Pour une installation SCCM, le fichier cert.pem doit résider dans le dossier VRMGuestAgent.
- Pour les installations Linux de vSphere, le fichier cert.pem doit résider dans le dossier /usr/share/gugent.

Remarque Vous avez la possibilité d'installer des logiciels et des agents invités ensemble en téléchargeant le script suivant depuis <https://APPLIANCE/software/index.html>. Le script permet de traiter l'acceptation des empreintes digitales du certificat SSL pendant la création des modèles.

- Linux

```
prepare_vra_template.sh
```

- Windows

```
prepare_vra_template.ps1
```

Si vous installez le logiciel et l'agent invité en même temps, vous pouvez ignorer les instructions de [Installer l'agent invité sur une machine de référence Linux](#) ou [Installer l'agent invité sur une machine de référence Windows](#).

Installer l'agent invité sur une machine de référence Linux

Installez l'agent invité Linux sur vos machines de référence pour personnaliser davantage les machines après le déploiement.

Prérequis

- Identifiez ou créez la machine de référence.
- Les fichiers d'agent invité que vous téléchargez contiennent les formats de module tar.gz et RPM. Si votre système d'exploitation ne peut pas installer les fichiers tar.gz ou RPM, utilisez un outil de conversion pour convertir les fichiers d'installation dans le format de module que vous préférez.
- Établissez une confiance sécurisée entre l'agent invité et votre machine Manager Service. Reportez-vous à [Configurer l'agent invité pour approuver un serveur](#).

Procédure

- 1 Accédez à la page de la console de gestion du dispositif vRealize Automation.

Par exemple : <https://va-hostname.domain.com>.

- 2 Cliquez sur **Page des agents invités et logiciels** dans la section d'installation de composants vRealize Automation de la page.

Par exemple : `https://va-hostname.domain.com/software/index.html`.

La page **Programmes d'installation d'agents invités et logiciels** s'ouvre. Elle affiche des liens vers les téléchargements disponibles.

- 3 Cliquez sur **Modules d'agents invités Linux** dans la section des programmes d'installation d'agents invités de la page pour télécharger et enregistrer le fichier `LinuxGuestAgentPkgs.zip`.
- 4 Décompressez le fichier `LinuxGuestAgentPkgs.zip` téléchargé pour créer le répertoire `VraLinuxGuestAgent`.
- 5 Installez le module d'agent invité qui correspond au système d'exploitation invité que vous déployez lors du provisionnement.
 - a Accédez au sous-répertoire `VraLinuxGuestAgent` correspondant au système d'exploitation invité à déployer pendant le provisionnement, par exemple `rhel32`.
 - b Localisez le format de module que vous préférez ou convertissez un module dans le format de votre choix.
 - c Installez le module d'agent invité sur votre machine de référence.

Par exemple, pour installer les fichiers du module RPM, exécutez `rpm -i gurent-gurent-7.1.0-4201531.i386.rpm`.

- 6 Configurez l'agent invité pour qu'il communique avec Manager Service en exécutant `installgurent.sh Manager_Service_Hostname_fdsn:portnumber ssl platform`.

Le numéro de port par défaut pour Manager Service est 443. Les valeurs de plateforme acceptées sont `ec2`, `vcd`, `vca` et `vsphere`.

Option	Description
Si vous utilisez un équilibrage de charge	<p>Entrez le nom de domaine complet et le numéro de port de votre équilibrage de charge Manager Service. Par exemple :</p> <pre>cd /usr/share/gurent ./installgurent.sh load_balancer_manager_service.mycompany.com:443 ssl ec2</pre>
Sans équilibrage de charge	<p>Entrez le nom de domaine complet et le numéro de port de votre machine Manager Service. Par exemple :</p> <pre>cd /usr/share/gurent ./installgurent.sh manager_service_machine.mycompany.com:443 ssl vsphere</pre>

- 7 Si les machines déployées ne sont pas déjà configurées pour approuver le certificat SSL de Manager Service, vous devez installer le fichier `cert.pem` sur votre machine de référence pour établir la confiance.

- Pour l'approche la plus sécurisée, obtenez le certificat `cert.pem` et installez le fichier manuellement sur la machine de référence.
- Pour une approche plus pratique, vous pouvez connecter l'équilibrage de charge Manager Service ou la machine Manager Service et télécharger le certificat `cert.pem`.

Option	Description
Si vous utilisez un équilibrage de charge	<p>En tant qu'utilisateur racine sur la machine de référence, exécutez la commande suivante :</p> <pre>echo openssl s_client -connect manager_service_load_balancer.mycompany.com:443 sed -ne '/- BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > cert.pem</pre>
Sans équilibrage de charge	<p>En tant qu'utilisateur racine sur la machine de référence, exécutez la commande suivante :</p> <pre>echo openssl s_client -connect manager_service_machine.mycompany.com:443 sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > cert.pem</pre>

- 8 Si vous installez l'agent invité sur un système d'exploitation Ubuntu, créez des liens symboliques pour les objets partagés en exécutant un des ensembles de commandes suivants.

Option	Description
systèmes 64 bits	<pre>cd /lib/x86_64-linux-gnu sudo ln -s libssl.so.1.0.0 libssl.so.10 sudo ln -s libcrypto.so.1.0.0 libcrypto.so.10</pre>
systèmes 32 bits	<pre>cd /lib/i386-linux-gnu sudo ln -s libssl.so.1.0.0 libssl.so.10 sudo ln -s libcrypto.so.1.0.0 libcrypto.so.10</pre>

Suivant

Convertissez votre machine de référence en modèle pour le clonage, une image de machine Amazon ou un snapshot que vos architectes IaaS peuvent utiliser lors de la création de Blueprints.

Installer l'agent invité sur une machine de référence Windows

Installez l'agent invité Windows vRealize Automation sur une machine de référence Windows afin de l'exécuter en tant que service Windows et de permettre une personnalisation plus poussée des machines.

Prérequis

- Identifiez ou créez la machine de référence.

- Établissez une confiance sécurisée entre l'agent invité et votre machine Manager Service. Reportez-vous à [Configurer l'agent invité pour approuver un serveur](#).

Procédure

- 1 Accédez à la page **Programmes d'installation de l'agent invité et de l'agent logiciel** du dispositif vRealize Automation :

`https://vrealize-automation-appliance-FQDN/software`

- 2 Sous **Programmes d'installation de l'agent invité**, téléchargez et enregistrez le fichier exécutable 32 bits ou 64 bits à la racine du lecteur C:.

Remarque Il existe une solution de remplacement par ligne de commande pour cette procédure d'installation de l'agent invité. Au lieu de télécharger les exécutables, vous pouvez accéder aux **Programmes d'installation de logiciels Windows** sur la page Programmes d'installation d'agent logiciel et invité. Vous pouvez y télécharger et y exécuter le script PowerShell `prepare_vra_template.ps1`:

```
PowerShell -NoProfile -ExecutionPolicy Bypass -Command prepare_vra_template.ps1
```

- 3 Extrayez les fichiers d'agent invité Windows en exécutant le fichier exécutable.

L'extraction crée C:\VRMGuestAgent et ajoute les fichiers.

Ne renommez pas C:\VRMGuestAgent.

- 4 Configurez l'agent invité pour qu'il communique avec Manager Service.

a Ouvrez une invite de commande élevée.

b Accédez à C:\VRMGuestAgent.

c Placez le fichier PEM de Manager Service approuvé dans le répertoire C:\VRMGuestAgent\ pour configurer l'agent invité pour qu'il approuve votre machine Manager Service.

d Exécutez `winservice -i -h Manager_Service_Hostname_fqdn:portnumber -p ssl`.

Le numéro de port par défaut pour Manager Service est 443.

Option	Description
Si vous utilisez un équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de votre équilibrage de charge Manager Service. Par exemple, <code>winservice -i -h load_balancer_manager_service.mycompany.com:443 -p ssl</code> .
Sans équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de votre machine Manager Service. Par exemple, <code>winservice -i -h manager_service_machine.mycompany.com:443 -p ssl</code> .
Si vous préparez une image de machine Amazon	Vous devez spécifier que vous utilisez Amazon. Par exemple, <code>winservice -i -h manager_service_machine.mycompany.com:443:443 -p ssl -c ec2</code>

Le nom du service Windows est VCACGuestAgentService. Pour obtenir le fichier d'installation, accédez à VCAC-GuestAgentService.log dans l'annuaire C:\VRMGuestAgent.

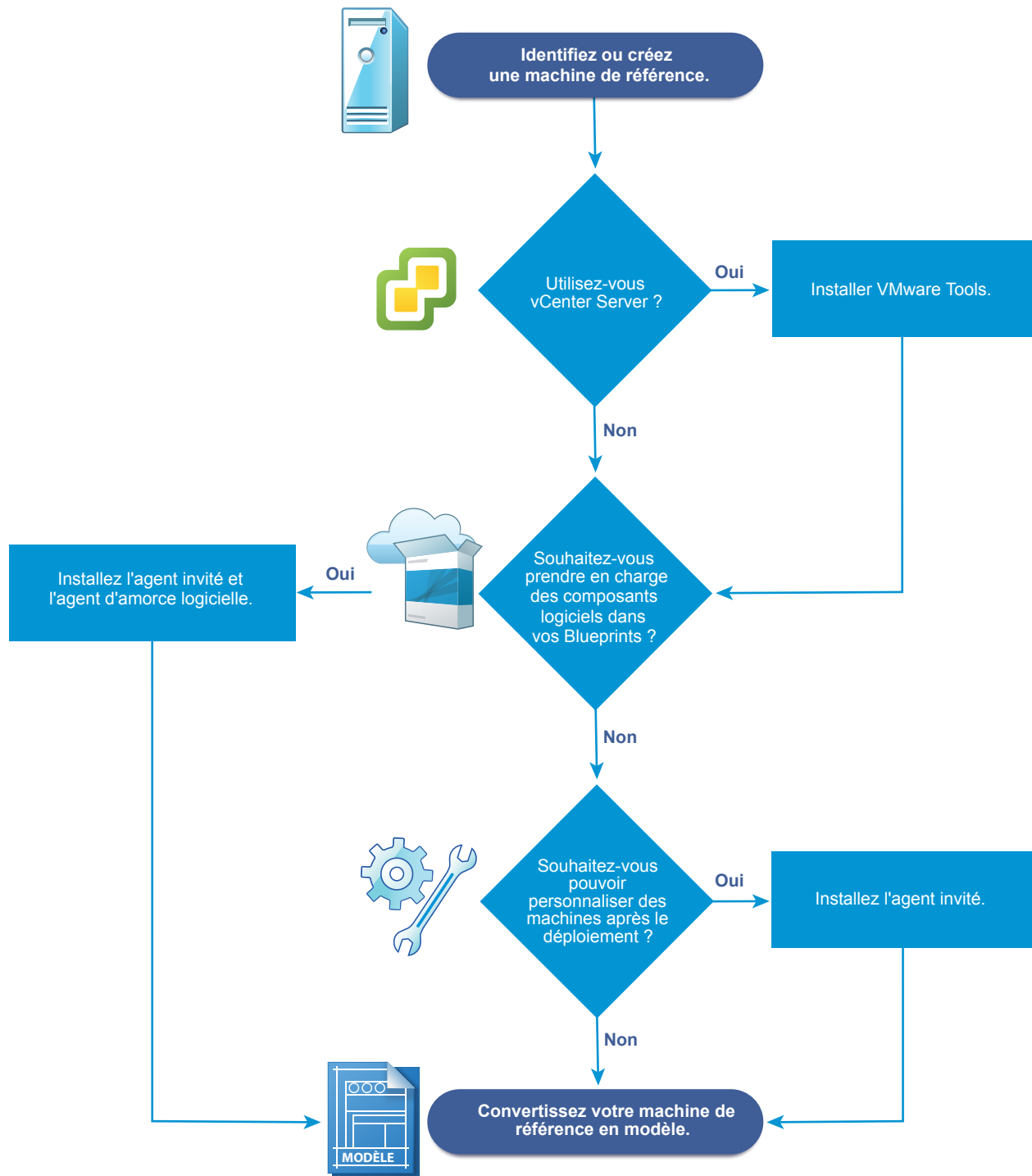
Suivant

Convertissez votre machine de référence en modèle pour le clonage, en image de machine Amazon ou en snapshot afin que vos architectes IaaS puissent utiliser votre modèle lors de la création de Blueprints.

Liste de vérification pour la préparation du provisionnement par le clonage

Il vous faut effectuer quelque préparation hors de vRealize Automation pour créer un modèle et les objets de personnalisation utilisés pour cloner les machines virtuelles Linux et Windows.

Le clonage nécessite un modèle sur lequel baser le clonage, créé à partir d'une machine de référence.



Si vous provisionnez une machine Windows par le biais du clonage, la seule manière d'associer la machine provisionnée à un domaine Active Directory consiste à utiliser la spécification de personnalisation de vCenter Server ou à inclure le profil du système d'exploitation invité à votre modèle SCVMM. Les machines provisionnées par clonage ne peuvent pas être placées dans un conteneur Active Directory pendant le provisionnement. Vous devez faire cela manuellement après le provisionnement.

Tableau 1-8. Liste de vérification pour la préparation du provisionnement par le clonage

Tâche	Emplacement	Détails
<input type="checkbox"/> Identifiez ou créez la machine de référence.	Hyperviseur	Reportez-vous à la documentation fournie par votre hyperviseur.
<input type="checkbox"/> (Facultatif) Si vous souhaitez que votre modèle cloné prenne en charge les composants Logiciel, installez l'agent vRealize Automation invité et l'agent de démarrage logiciel sur votre machine de référence.	Machine de référence	Pour les machines de référence Windows, consultez Préparer une machine de référence Windows pour prendre en charge Logiciel . Pour les machines de référence Linux, consultez Préparer une machine de référence Linux pour prendre en charge Logiciel .
<input type="checkbox"/> (Facultatif) Si vous n'avez pas besoin que votre modèle cloné prenne en charge les composants Logiciel, mais que vous souhaitez avoir la possibilité de personnaliser les machines déployées, installez l'agent vRealize Automation invité sur votre machine de référence.	Machine de référence	Reportez-vous à Utilisation d'un agent invité vRealize Automation dans un provisionnement .
<input type="checkbox"/> Si vous travaillez dans un environnement vCenter Server, installez VMware Tools sur la machine de référence.	vCenter Server	Consultez la documentation de VMware Tools.
<input type="checkbox"/> Utilisez la machine de référence pour créer un modèle de clonage.	Hyperviseur	La machine de référence peut être mise sous ou hors tension. Si vous effectuez un clonage dans vCenter Server, vous pouvez utiliser directement une machine de référence sans créer de modèle. Reportez-vous à la documentation fournie par votre hyperviseur.
<input type="checkbox"/> Créez l'objet de personnalisation pour configurer des machines clonées en appliquant des informations de l'utilitaire de préparation du système ou une personnalisation Linux.	Hyperviseur	Si vous effectuez un clonage pour Linux, vous pouvez installer l'agent invité Linux et fournir des scripts de personnalisation externes plutôt que de créer un objet de personnalisation. Si vous effectuez un clonage avec vCenter Server, vous devez fournir la spécification de personnalisation comme objet de personnalisation. Reportez-vous à la documentation fournie par votre hyperviseur.
<input type="checkbox"/> Rassemblez les informations requises pour créer des Blueprints clonant votre modèle.	Capturez les informations et transférez-les à vos architectes d'IaaS.	Reportez-vous à Feuille d'activité de la préparation du provisionnement virtuel par clonage .

Feuille d'activité de la préparation du provisionnement virtuel par clonage

Complétez la feuille d'activité du transfert des connaissances afin de noter des informations relatives au modèle, aux personnalisations et aux propriétés personnalisées requis à la création de Blueprints de clone, pour les modèles que vous avez préparés dans l'environnement. Cependant, toutes ces informations ne sont pas obligatoires pour chaque implémentation. Servez-vous de cette feuille d'activité comme d'un guide. Vous pouvez également copier ses tableaux et les coller dans un outil de traitement de texte pour les modifier selon vos besoins.

Informations requises sur le modèle et la réservation

Tableau 1-9. Feuille d'activité sur les informations relatives au modèle et à la réservation

Informations requises	Ma valeur	Détails
Nom du modèle		
Réservations dans lesquelles le modèle est disponible ou dans lesquelles une stratégie de réservation doit s'appliquer		Pour éviter les erreurs pendant le provisionnement, assurez-vous que le modèle est disponible sur toutes les réservations. Autrement, créez des stratégies de réservation que les architectes peuvent utiliser pour limiter le Blueprint aux réservations dans lesquelles le modèle est disponible.
(vSphere uniquement) Type de clonage demandé pour ce modèle		<ul style="list-style-type: none"> ■ Cloner ■ Clone lié ■ NetApp FlexClone
Nom de la spécification de personnalisation (requis pour le clonage avec des adresses IP statiques)		Vous ne pouvez pas réaliser de personnalisations de machines Windows sans un objet de spécification de personnalisation.
(SCVMM uniquement) Nom ISO		
(SCVMM uniquement) Disque dur virtuel		
(SCVMM uniquement) Profil matériel à attacher aux machines provisionnées		

Groupes de propriétés requis

Vous pouvez remplir les sections d'informations relatives aux propriétés personnalisées de la feuille d'activité. Vous pouvez également créer des groupes de propriétés et demander aux architectes d'ajouter ces groupes à leurs Blueprints, au lieu de procéder propriété par propriété.

Système d'exploitation vCenter Server requis

Vous devez appliquer la propriété de personnalisation du système d'exploitation pour le provisionnement de vCenter Server.

Tableau 1-10. Système d'exploitation vCenter Server

Propriété personnalisée	Ma valeur	Description
VMware.VirtualCenter.OperatingSystem		Spécifie la version du système d'exploitation invité vCenter Server (VirtualMachineGuestOsIdentifier) avec laquelle vCenter Server crée la machine. Cette version de système d'exploitation doit correspondre à la version du système d'exploitation qui sera installé sur la machine provisionnée. Les administrateurs peuvent créer des groupes de propriétés en utilisant un des différents ensembles de propriétés, VMware[OS_Version]Properties par exemple, qui sont prédéfinis pour inclure les valeurs VMware.VirtualCenter.OperatingSystem correctes. Cette propriété s'applique au provisionnement virtuel.

Informations relatives aux scripts Visual Basic

Si vous avez configuré vRealize Automation pour qu'il exécute les scripts Visual Basic en tant qu'étapes supplémentaires du cycle de vie de la machine, vous devez inclure au Blueprint des informations sur ces scripts.

Remarque Un administrateur Fabric peut créer un groupe de propriétés en utilisant les jeux de propriétés ExternalPreProvisioningVbScript et ExternalPostProvisioningVbScript pour fournir les informations requises. Cela permet aux architectes du Blueprint d'inclure facilement et correctement ces informations à leurs Blueprints.

Tableau 1-11. Informations relatives aux scripts Visual Basic

Propriété personnalisée	Ma valeur	Description
ExternalPreProvisioningVbScript		Exécutez un script avant le provisionnement. Entrez le chemin complet du script, y compris le nom du fichier et son extension. %System Drive %Program Files (x86)\VMware\vCAC Agents\EPI_Agents\Scripts\SendEmail.vbs
ExternalPostProvisioningVbScript		Exécutez un script après le provisionnement. Entrez le chemin complet du script, y compris le nom du fichier et son extension. %System Drive %Program Files (x86)\VMware\vCAC Agents\EPI_Agents\Scripts\SendEmail.vbs

Informations relatives au script de personnalisation de l'agent Linux invité

Si vous avez configuré le modèle Linux afin qu'il utilise l'agent invité pour exécuter des scripts de personnalisation, vous devez inclure au Blueprint des informations sur ces scripts.

Tableau 1-12. Feuille d'activité sur les informations relatives au script de personnalisation de l'agent Linux invité

Propriété personnalisée	Ma valeur	Description
Linux.ExternalScript.Name		<p>Spécifie le nom d'un script de personnalisation optionnel, par exemple <code>config.sh</code>, que l'agent invité Linux exécute une fois que le système d'exploitation a été installé. Cette propriété est disponible pour les machines Linux clonées à partir des modèles sur lesquels l'agent Linux est installé.</p> <p>Si vous spécifiez un script externe, vous devez également définir son emplacement en utilisant les propriétés <code>Linux.ExternalScript.LocationType</code> et <code>Linux.ExternalScript.Path</code>.</p>
Linux.ExternalScript.LocationType		<p>Spécifie le type d'emplacement du script de personnalisation nommé dans la propriété <code>Linux.ExternalScript.Name</code>. Le type d'emplacement peut être <code>local</code> ou <code>nfs</code>.</p> <p>Vous devez également spécifier l'emplacement du script en utilisant la propriété <code>Linux.ExternalScript.Path</code>. Si le type d'emplacement est <code>nfs</code>, utilisez également la propriété <code>Linux.ExternalScript.Server</code>.</p>
Linux.ExternalScript.Server		<p>Spécifie le nom du serveur NFS, par exemple <code>lab-ad.lab.local</code>, sur lequel le script de personnalisation externe Linux nommé dans <code>Linux.ExternalScript.Name</code> est situé.</p>
Linux.ExternalScript.Path		<p>Spécifie le chemin d'accès local au script de personnalisation Linux ou le chemin d'exportation vers la personnalisation Linux sur le serveur NFS. La valeur doit commencer par une barre oblique et ne doit pas inclure le nom du fichier, par exemple <code>/scripts/linux/config.sh</code>.</p>

Autres propriétés de personnalisation de l'agent invité

Si vous avez installé l'agent invité sur la machine de référence, vous pouvez utiliser les propriétés de personnalisation pour personnaliser davantage les machines après le déploiement.

Tableau 1-13. Feuille d'activité sur les propriétés personnalisées pour personnaliser les machines clonées avec un agent invité

Propriété personnalisée	Ma valeur	Description
VirtualMachine.Admin.AddOwnerToAdmins		Définissez cette propriété sur True (valeur par défaut) pour ajouter le propriétaire de la machine, spécifié par la propriété VirtualMachine.Admin.Owner, au groupe d'administrateurs local sur la machine.
VirtualMachine.Admin.AllowLogin		Définissez cette propriété sur True (valeur par défaut) pour ajouter le propriétaire de la machine au groupe d'utilisateurs du bureau à distance local, spécifié par la propriété VirtualMachine.Admin.Owner.
VirtualMachine.Admin.UseGuestAgent		Si l'agent invité est installé en tant que service sur un modèle pour le clonage, définissez cette propriété sur True dans le Blueprint de machine pour activer le service d'agent invité sur les machines clonées à partir de ce modèle. Lors du démarrage de la machine, le service d'agent invité est démarré. Pour désactiver l'agent invité, définissez cette propriété sur False. Si elle est définie sur False, le workflow de clone amélioré n'utilisera pas l'agent invité pour les tâches du système d'exploitation invité, réduisant sa fonctionnalité au paramètre VMwareCloneWorkflow. Si cette propriété n'est pas spécifiée ou si elle est définie sur une autre valeur que False, le workflow de clone amélioré envoie les éléments de travail à l'agent invité.
VirtualMachine.DiskN.Active		Définissez cette propriété sur True (valeur par défaut) pour spécifier que le disque de machine N est actif. Définissez cette propriété sur False pour spécifier que le disque de machine N n'est pas actif.

Tableau 1-13. Feuille d'activité sur les propriétés personnalisées pour personnaliser les machines clonées avec un agent invité (suite)

Propriété personnalisée	Ma valeur	Description
<code>VirtualMachine.DiskN.Size</code>		<p>Définit la taille en Go du disque <i>N</i>. Par exemple, pour donner une taille de 150 Go à un disque G, définissez la propriété personnalisée <code>VirtualMachine.Disk0.Size</code> et entrez la valeur 150. La numérotation des disques doit être séquentielle. Par défaut, une machine comporte un disque identifié par <code>VirtualMachine.Disk0.Size</code>, où la taille est spécifiée par la valeur de stockage dans le Blueprint à partir duquel la machine est provisionnée. La valeur de stockage sur l'interface utilisateur du Blueprint remplace la valeur dans la propriété <code>VirtualMachine.Disk0.Size</code>. La propriété <code>VirtualMachine.Disk0.Size</code> n'est pas disponible comme propriété personnalisée en raison de sa relation avec l'option de stockage sur le Blueprint. Des disques supplémentaires peuvent être ajoutés en spécifiant <code>VirtualMachine.Disk1.Size</code>, <code>VirtualMachine.Disk2.Size</code>, etc. <code>VirtualMachine.Admin.TotalDiskUsage</code> représente toujours le total des propriétés <code>.DiskN.Size</code> plus l'allocation de taille <code>VMware.Memory.Reservation</code>.</p>
<code>VirtualMachine.DiskN.Label</code>		<p>Spécifie le nom d'un disque de machine <i>N</i>. La longueur maximale du nom du disque est de 32 caractères. La numérotation des disques doit être séquentielle. Lorsqu'elle est utilisée avec un agent invité, elle spécifie l'étiquette d'un disque de machine <i>N</i> au sein du système d'exploitation invité.</p>
<code>VirtualMachine.DiskN.Letter</code>		<p>Spécifie la lettre de lecteur ou le point de montage du disque d'une machine <i>N</i>. La valeur par défaut est C. Par exemple, pour spécifier la lettre D pour le disque 1, définissez la propriété personnalisée sur <code>VirtualMachine.Disk1.Letter</code> et entrez la valeur D. La numérotation des disques doit être séquentielle. Lorsqu'elle est utilisée conjointement avec un agent invité, cette valeur spécifie la lettre de lecteur ou le point de montage sous lequel un disque supplémentaire <i>N</i> est monté par l'agent invité dans le système d'exploitation hôte.</p>

Tableau 1-13. Feuille d'activité sur les propriétés personnalisées pour personnaliser les machines clonées avec un agent invité (suite)

Propriété personnalisée	Ma valeur	Description
VirtualMachine.Admin.CustomizeGuestOSDelay		Spécifie la durée d'attente après le provisionnement et avant de démarrer la personnalisation du système d'exploitation invité. Cette valeur doit être dans le format HH:MM:SS. Si la propriété n'est pas définie, la valeur par défaut est une minute (00:01:00). Si vous choisissez de ne pas inclure cette propriété personnalisée, le provisionnement peut échouer si la machine virtuelle redémarre avant que les éléments de travail de l'agent invité soient terminés, ce qui entraîne l'échec du provisionnement.
VirtualMachine.Customize.WaitComplete		Définissez cette propriété sur True pour empêcher le workflow de provisionnement d'envoyer des éléments de travail à l'agent invité tant que toutes les personnalisations ne sont pas terminées.
VirtualMachine.SoftwareN.Name		Spécifie le nom descriptif d'une application logicielle <i>N</i> ou d'un script d'installation ou d'exécution lors du provisionnement. Cette propriété est facultative et sert uniquement à des fins d'information. Elle ne remplit aucune fonction réelle pour le workflow de clone amélioré ou l'agent invité, mais elle est utile pour une sélection de logiciels personnalisée dans une interface utilisateur ou pour les rapports d'utilisation des logiciels.
VirtualMachine.SoftwareN.ScriptPath		<p>Spécifie le chemin d'accès complet à un script d'installation d'application. Le chemin doit être un chemin absolu valide tel qu'il est détecté par le système d'exploitation invité et doit inclure le nom d'un fichier de script.</p> <p>Vous pouvez transmettre les valeurs de propriété personnalisée comme paramètres au script en insérant <code>{CustomPropertyName}</code> dans la chaîne du chemin d'accès. Par exemple, si vous avez une propriété personnalisée appelée <code>ActivationKey</code> dont la valeur est 1234, le chemin d'accès au script est <code>D:\InstallApp.bat -key {ActivationKey}</code>. L'agent invité exécute la commande <code>D:\InstallApp.bat -key 1234</code>. Votre fichier de script peut alors être planifié pour accepter et utiliser cette valeur.</p>

Tableau 1-13. Feuille d'activité sur les propriétés personnalisées pour personnaliser les machines clonées avec un agent invité (suite)

Propriété personnalisée	Ma valeur	Description
VirtualMachine.SoftwareN.ISOName		Spécifie le chemin d'accès et le nom du fichier ISO par rapport à la racine de la banque de données. Le format est <i>/nom_fichier/nom_sous-dossier/nom_fichier.iso</i> . Si aucune valeur n'est spécifiée, le fichier ISO n'est pas monté.
VirtualMachine.SoftwareN.ISOLocation		Spécifie le chemin de stockage contenant le fichier image ISO qui doit être utilisé par l'application ou le script. Formatez le chemin d'accès tel qu'il apparaît dans la réservation d'hôte, par exemple <i>netapp-1:it_nfs_1</i> . Si aucune valeur n'est spécifiée, le fichier ISO n'est pas monté.

Propriétés personnalisées de mise en réseau

Vous pouvez spécifier la configuration de dispositifs réseau spécifiques sur une machine en utilisant des propriétés personnalisées.

Les propriétés personnalisées associées à la mise en réseau courantes sont répertoriées dans le tableau suivant. Pour des propriétés personnalisées supplémentaires et associées, reportez-vous aux rubriques *Propriétés personnalisées pour des Blueprints de clone* et *Propriétés personnalisées pour la mise en réseau* dans *Référence des propriétés personnalisées*.

Tableau 1-14. Propriétés personnalisées pour la configuration de la mise en réseau

Propriété personnalisée	Ma valeur	Description
VirtualMachine.NetworkN.Addresses		Spécifie l'adresse IP du périphérique réseau <i>N</i> dans une machine provisionnée avec une adresse IP statique.
VirtualMachine.NetworkN.MacAddressType		<p>Indique si l'adresse MAC du périphérique réseau <i>N</i> est générée ou définie par l'utilisateur (statique). Cette propriété est disponible pour le clonage. La valeur par défaut est générée. Si la valeur est statique, vous devez également utiliser <code>VirtualMachine.NetworkN.MacAddress</code> pour spécifier l'adresse MAC.</p> <p>Les propriétés personnalisées <code>VirtualMachine.NetworkN</code> sont spécifiques aux Blueprints et aux machines individuels. Lorsqu'une machine est demandée, l'allocation de réseau et d'adresse IP est effectuée avant que la machine soit attribuée à une réservation. Étant donné qu'il n'est pas garanti que les Blueprints soient alloués à une réservation spécifique, n'utilisez pas cette propriété dans une réservation. Cette propriété n'est pas prise en charge pour les réseaux NAT ou acheminés à la demande.</p>

Tableau 1-14. Propriétés personnalisées pour la configuration de la mise en réseau (suite)

Propriété personnalisée	Ma valeur	Description
VirtualMachine.NetworkN.MacAddress		<p>Spécifie l'adresse MAC d'un périphérique réseau <i>N</i>. Cette propriété est disponible pour le clonage.</p> <p>Si la valeur de VirtualMachine.NetworkN.MacAddressType est générée, cette propriété contient l'adresse générée.</p> <p>Si la valeur de VirtualMachine.NetworkN.MacAddressType est statique, cette propriété spécifie l'adresse MAC. Pour les machines provisionnées sur les hôtes de serveur ESX, l'adresse doit être dans la plage spécifiée par VMware. Pour des informations détaillées, reportez-vous à la documentation vSphere.</p> <p>Les propriétés personnalisées VirtualMachine.NetworkN sont spécifiques aux Blueprints et aux machines individuels. Lorsqu'une machine est demandée, l'allocation de réseau et d'adresse IP est effectuée avant que la machine soit attribuée à une réservation. Étant donné qu'il n'est pas garanti que les Blueprints soient alloués à une réservation spécifique, n'utilisez pas cette propriété dans une réservation. Cette propriété n'est pas prise en charge pour les réseaux NAT ou acheminés à la demande.</p>

Tableau 1-14. Propriétés personnalisées pour la configuration de la mise en réseau (suite)

Propriété personnalisée	Ma valeur	Description
VirtualMachine.NetworkN.Name		<p>Spécifie le nom du réseau auquel se connecter, par exemple le périphérique réseau <i>N</i> auquel une machine est associée. Cela est équivalent à une carte d'interface réseau (NIC).</p> <p>Par défaut, un réseau est attribué à partir des chemins d'accès réseau disponibles dans la réservation dans laquelle la machine est provisionnée. Voir aussi <code>VirtualMachine.NetworkN.AddressType</code> et <code>VirtualMachine.NetworkN.ProfileName</code>.</p> <p>Vous pouvez vous assurer qu'un périphérique réseau est connecté à un réseau spécifique en définissant la valeur de cette propriété sur le nom d'un réseau dans une réservation disponible. Par exemple, si vous attribuez des propriétés pour <i>N</i>= 0 et 1, vous obtenez 2 cartes réseau et leur valeur attribuée, à condition que le réseau soit sélectionné dans la réservation associée.</p> <p>Les propriétés personnalisées <code>VirtualMachine.NetworkN</code> sont spécifiques aux Blueprints et aux machines. Lorsqu'une machine est demandée, l'allocation de réseau et d'adresse IP est effectuée avant que la machine soit attribuée à une réservation. Étant donné qu'il n'est pas garanti que les Blueprints soient alloués à une réservation spécifique, n'utilisez pas cette propriété dans une réservation. Cette propriété n'est pas prise en charge pour les réseaux NAT ou acheminés à la demande.</p> <p>Pour obtenir un exemple d'utilisation de cette propriété personnalisée pour définir dynamiquement <code>VirtualMachine.Network0.Name</code> sur la base d'une sélection de consommateur dans une liste de réseaux disponibles prédéfinis, consultez le blog Ajout d'une liste déroulante de sélection de réseau dans vRA 7.</p>

Tableau 1-14. Propriétés personnalisées pour la configuration de la mise en réseau (suite)

Propriété personnalisée	Ma valeur	Description
VirtualMachine.NetworkN.PortID		<p>Spécifie l'ID de port qui doit être utilisé pour le périphérique réseau <i>N</i> lorsqu'un groupe dvPort est utilisé avec un commutateur distribué vSphere.</p> <p>Les propriétés personnalisées VirtualMachine.NetworkN sont spécifiques aux Blueprints et aux machines individuels. Lorsqu'une machine est demandée, l'allocation de réseau et d'adresse IP est effectuée avant que la machine soit attribuée à une réservation. Étant donné qu'il n'est pas garanti que les Blueprints soient alloués à une réservation spécifique, n'utilisez pas cette propriété dans une réservation. Cette propriété n'est pas prise en charge pour les réseaux NAT ou acheminés à la demande.</p>
VirtualMachine.NetworkN.ProfileName et VirtualMachine.NetworkN.NetworkProfileName		<p>Spécifie le nom d'un profil réseau à partir duquel une adresse IP statique doit être attribuée au périphérique réseau <i>N</i> ou à partir duquel obtenir la plage d'adresses IP statiques pouvant être attribuée au périphérique réseau <i>N</i> d'une machine clonée, où <i>N</i>=0 pour le premier périphérique, 1 pour le second, etc.</p> <ul style="list-style-type: none"> ■ VirtualMachine.NetworkN.ProfileName permet de sélectionner un réseau à partir de la réservation qu'il dispose ou non d'un profil réseau correspondant. ■ Utilisez VirtualMachine.NetworkN.NetworkProfileName pour sélectionner uniquement les réseaux qui disposent d'un profil réseau correspondant portant le même nom. <p>Le profil réseau désigné par la propriété est utilisé pour allouer une adresse IP. Toutefois, la machine provisionnée est associée à un réseau quelconque sélectionné dans la réservation à l'aide d'un modèle de type Round-robin.</p>

Tableau 1-14. Propriétés personnalisées pour la configuration de la mise en réseau (suite)

Propriété personnalisée	Ma valeur	Description
<ul style="list-style-type: none"> VirtualMachine.NetworkN.SubnetMask VirtualMachine.NetworkN.Gateway VirtualMachine.NetworkN.PrimaryDns VirtualMachine.NetworkN.SecondaryDns VirtualMachine.NetworkN.PrimaryWins VirtualMachine.NetworkN.SecondaryWins VirtualMachine.NetworkN.DnsSuffix VirtualMachine.NetworkN.DnsSearchSuffixes 		<p>L'ajout d'un nom vous permet de créer plusieurs versions d'une propriété personnalisée. Par exemple, les propriétés suivantes peuvent répertorier des pools d'équilibrage de charge définis pour une utilisation générale et des machines avec des exigences de performances élevées, modérées et faibles :</p> <ul style="list-style-type: none"> VCNS.LoadBalancerEdgePool.Names VCNS.LoadBalancerEdgePool.Names.moderate VCNS.LoadBalancerEdgePool.Names.high VCNS.LoadBalancerEdgePool.Names.low <p>Configure les attributs du profil réseau spécifié dans VirtualMachine.NetworkN.ProfileName.</p>
VCNS.LoadBalancerEdgePool.Names.nom		<p>Spécifie les pools d'équilibrage de charge NSX auxquels la machine virtuelle est attribuée lors du provisionnement. La machine virtuelle est attribuée à tous les ports de service de tous les pools spécifiés. La valeur est un nom <i>edge/pool</i> ou une liste de noms <i>edge/pool</i> séparés par des virgules. Les noms sont sensibles à la casse.</p> <p>L'ajout d'un nom vous permet de créer plusieurs versions d'une propriété personnalisée. Par exemple, les propriétés suivantes peuvent répertorier des pools d'équilibrage de charge définis pour une utilisation générale et des machines avec des exigences de performances élevées, modérées et faibles :</p> <ul style="list-style-type: none"> VCNS.LoadBalancerEdgePool.Names VCNS.LoadBalancerEdgePool.Names.moderate VCNS.LoadBalancerEdgePool.Names.high VCNS.LoadBalancerEdgePool.Names.low

Tableau 1-14. Propriétés personnalisées pour la configuration de la mise en réseau (suite)

Propriété personnalisée	Ma valeur	Description
VCNS.SecurityGroup.Names. <i>nom</i>		<p>Spécifie le ou les groupes de sécurité NSX auxquels la machine virtuelle est attribuée lors du provisionnement. La valeur est un nom de groupe de sécurité ou une liste de noms séparés par des virgules. Les noms sont sensibles à la casse.</p> <p>L'ajout d'un nom vous permet de créer plusieurs versions de la propriété, qui peuvent être utilisées séparément ou conjointement. Par exemple, les propriétés suivantes peuvent répertorier des groupes de sécurité destinés à une utilisation générale, pour le personnel commercial et pour le support :</p> <ul style="list-style-type: none"> ■ VCNS.SecurityGroup.Names ■ VCNS.SecurityGroup.Names.sale s ■ VCNS.SecurityGroup.Names.support
VCNS.SecurityTag.Names. <i>nom</i>		<p>Spécifie la ou les balises de sécurité NSX auxquelles la machine virtuelle est associée lors du provisionnement. La valeur est un nom de balise de sécurité ou une liste de noms séparés par des virgules. Les noms sont sensibles à la casse.</p> <p>L'ajout d'un nom vous permet de créer plusieurs versions de la propriété, qui peuvent être utilisées séparément ou conjointement. Par exemple, les propriétés suivantes peuvent répertorier des balises de sécurité destinées à une utilisation générale, pour le personnel commercial et pour le support :</p> <ul style="list-style-type: none"> ■ VCNS.SecurityTag.Names ■ VCNS.SecurityTag.Names.sales ■ VCNS.SecurityTag.Names.support

Préparation pour le provisionnement vCloud Air et vCloud Director

Pour préparer le provisionnement de machines vCloud Air et vCloud Director avec vRealize Automation, vous devez configurer le centre de données virtuel de l'organisation avec des modèles et des objets de personnalisation.

Pour provisionner des ressources vCloud Air et vCloud Director avec vRealize Automation, l'organisation nécessite un modèle à partir duquel cloner consistant en une ou plusieurs ressources machine.

Les modèles à partager entre les organisations doivent être publics. Seuls les modèles réservés sont disponibles pour vRealize Automation comme sources de clonage.

Remarque Lorsque vous créez un Blueprint par clonage depuis un modèle, l'identifiant unique de ce modèle se retrouve associé au Blueprint. Lorsque le Blueprint est publié dans le vRealize Automation catalogue et utilisé au cours des processus de provisionnement et de collecte de données, le modèle associé est reconnu. Si vous supprimez le modèle de vCloud Air ou de vCloud Director, le provisionnement vRealize Automation et la collecte de données suivants échouent, car le modèle associé n'existe plus. Plutôt que de supprimer et de recréer un modèle, par exemple pour télécharger une version mise à jour, remplacez le modèle à l'aide du processus de remplacement de modèle vCloud Air vCloud Director. L'utilisation de vCloud Air ou de vCloud Director pour remplacer le modèle, plutôt que de supprimer et de recréer le modèle, conserve l'ID unique du modèle intact et permet que le provisionnement et la collecte de données continuent de fonctionner.

La présentation suivante illustre la procédure à suivre avant que vous utilisiez vRealize Automation pour créer des points de terminaison et définir des réservations et des Blueprints. Pour plus d'informations sur ces tâches administratives, reportez-vous à la documentation du produit vCloud Air et vCloud Director.

- 1 Dans vCloud Air ou vCloud Director, créez un modèle pour le clonage et ajoutez-le au catalogue de l'organisation.
- 2 Dans vCloud Air ou vCloud Director, utilisez le modèle pour spécifier des paramètres personnalisés comme mots de passe, domaine et scripts pour le système d'exploitation invité de chaque machine.

Vous pouvez utiliser vRealize Automation pour remplacer certains de ces paramètres.

La personnalisation peut varier selon le système d'exploitation invité de la ressource.

- 3 Dans vCloud Air ou vCloud Director, configurez le catalogue à partager avec tous les utilisateurs de l'organisation.

Dans vCloud Air ou vCloud Director, configurez un accès d'administrateur de comptes aux organisations applicables pour permettre à tous les utilisateurs et groupes de l'organisation d'accéder au catalogue. Sans cette désignation de partage, les modèles du catalogue ne sont pas visibles des architectes de points de terminaison ou de Blueprints dans vRealize Automation.

- 4 Réunissez les informations suivantes pour les inclure dans les Blueprints :
 - Nom du modèle vCloud Air ou vCloud Director.
 - Quantité d'espace de stockage spécifiée pour le modèle.

Préparation du provisionnement Kickstart Linux

Le provisionnement Kickstart Linux utilise un fichier de configuration permettant d'automatiser une installation Linux sur une machine provisionnée récemment. Pour préparer le provisionnement, vous devez créer une image ISO de démarrage et un fichier de configuration Kickstart ou autoYaST.

La présentation de niveau supérieur de la procédure requise pour préparer le provisionnement Kickstart Linux est la suivante :

- 1 Vérifier qu'un serveur DHCP est disponible sur le réseau. vRealize Automation ne peut pas provisionner de machines à l'aide du provisionnement Kickstart Linux, sauf si le DHCP est disponible.
- 2 Préparez le fichier de configuration. Dans le fichier de configuration, vous devez spécifier les emplacements du serveur vRealize Automation et le package d'installation de l'agent Linux. Reportez-vous à [Préparer l'exemple de fichier de configuration Kickstart Linux](#).
- 3 Modifiez `isolinux/isolinux.cfg` ou `loader/isolinux.cfg` pour spécifier le nom et l'emplacement du fichier de configuration et de la source de distribution Linux appropriée.
- 4 Créez l'image ISO de démarrage enregistrez-la à l'emplacement requis par votre plate-forme de virtualisation. Pour plus d'informations sur l'emplacement requis, reportez-vous à la documentation fournie par votre hyperviseur.
- 5 (Facultatif) Ajoutez des scripts de personnalisation.
 - a Pour spécifier des scripts de personnalisation d'installation dans le fichier de configuration, reportez-vous à la section [Spécifiez des scripts personnalisés dans un fichier de configuration kickstart ou autoYaST](#).
 - b Pour appeler des scripts Visual Basic dans un Blueprint, reportez-vous la section [Liste de contrôle pour l'exécution de scripts Visual Basic lors du provisionnement](#).
- 6 Réunissez les informations suivantes pour que les architectes du Blueprint puissent les inclure dans leurs Blueprints :
 - a Le nom et l'emplacement de l'image ISO.
 - b Pour les intégrations avec vCenter Server, la version du système d'exploitation invité de vCenter Server avec lequel vCenter Server doit créer la machine.

Remarque Vous pouvez créer un groupe de propriétés avec un ensemble de propriétés `BootIsoProperties` pour inclure les informations ISO requises. Cela permet d'inclure facilement ces informations correctement aux Blueprints.

Préparer l'exemple de fichier de configuration Kickstart Linux

vRealize Automation fournit des exemples de fichiers de configuration que vous pouvez modifier pour les adapter à vos besoins. Plusieurs modifications sont requises pour rendre les fichiers utilisables.

Procédure

- 1 Accédez à la page de la console de gestion du dispositif vRealize Automation.

Par exemple : `https://va-hostname.domain.com`.

- 2 Cliquez sur **Page des agents invités et logiciels** dans la section d'installation de composants vRealize Automation de la page.

Par exemple : `https://va-hostname.domain.com/software/index.html`.

La page **Programmes d'installation d'agents invités et logiciels** s'ouvre. Elle affiche des liens vers les téléchargements disponibles.

- 3 Cliquez sur **Modules d'agents invités Linux** dans la section des programmes d'installation d'agents invités de la page pour télécharger et enregistrer le fichier `LinuxGuestAgentPkgs.zip`.
- 4 Décompressez le fichier `LinuxGuestAgentPkgs.zip` téléchargé pour créer le répertoire `VraLinuxGuestAgent`.
- 5 Accédez au sous-répertoire `VraLinuxGuestAgent` correspondant au système d'exploitation invité à déployer pendant le provisionnement.
Par exemple : `rhel32`.
- 6 Ouvrez un fichier correspondant à votre système cible dans le sous-répertoire d'exemples, par exemple, `samples/sample-https-rhel6-x86.cfg`.
- 7 Remplacez toute les instances de la chaîne `host=dcac.example.net` par l'adresse IP ou le nom de domaine complet et le numéro de port de Manager Service ou de l'équilibrage de charge de Manager Service.

Plate-forme	Format requis
vSphere ESXi	Adresse IP, par exemple : <code>--host=172.20.9.59</code>
vSphere ESX	Adresse IP, par exemple : <code>--host=172.20.9.58</code>
SUSE 10	Adresse IP, par exemple : <code>--host=172.20.9.57</code>
Toutes les autres	Nom du domaine complet, par exemple : <code>--host=mycompany-host1.mycompany.local:443</code>

- 8 Recherchez chaque instance de `gugent.rpm` ou de `gugent.tar.gz` et remplacez l'URL `rpm.example.net` avec l'emplacement du package de l'agent invité.

Par exemple :

```
rpm -i nfs:172.20.9.59/suseagent/gugent.rpm
```

- 9 Enregistrez le fichier à un emplacement accessible aux machines provisionnées récemment.

Spécifiez des scripts personnalisés dans un fichier de configuration kickstart ou autoYaST

Vous pouvez modifier le fichier de configuration afin de copier ou d'installer des scripts personnalisés sur des machines provisionnées récemment. L'agent Linux exécute les scripts au point spécifié dans le workflow.

Votre script peut référencer l'un des fichiers `./properties.xml` des répertoires `/usr/share/gugent/site/workitem`.

Prérequis

- Préparez un fichier de configuration kickstart ou autoYaST. Reportez-vous à [Préparer l'exemple de fichier de configuration Kickstart Linux](#).
- Votre script doit renvoyer une valeur différente de zéro si le provisionnement de machines échoue.

Procédure

1 Créez ou identifiez le script que vous souhaitez utiliser.

2 Enregistrez le script en tant que *NN_scriptname*.

NN est un numéro à deux chiffres. Les scripts sont exécutés du numéro le plus petit au plus numéro le plus grand. Si deux scripts portent le même numéro, l'ordre est alphabétique, basé sur le *scriptname*.

3 Rendez votre script exécutable.

4 Recherchez la section postérieure à l'installation de votre fichier de configuration kickstart ou autoYaST.

Dans kickstart, cela est indiqué par `%post`. Dans autoYaST, cela est indiqué par `post-scripts`.

5 Modifiez la section postérieure à l'installation de votre fichier de configuration pour copier ou installer votre script dans le répertoire `/usr/share/gugent/site/workitem` de votre choix.

Les scripts personnalisés sont le plus souvent exécutés pour les kickstart/autoYaST virtuels avec les éléments de travail SetupOS (pour créer le provisionnement) et CustomizeOS (pour cloner le provisionnement), mais vous pouvez exécuter des scripts à tout moment du workflow.

Par exemple, vous pouvez modifier le fichier de configuration pour copier le script `11_addusers.sh` dans le répertoire `/usr/share/gugent/site/SetupOS` sur une machine provisionnée récemment à l'aide de la commande suivante :

```
cp nfs:172.20.9.59/linuxscripts/11_addusers.sh /usr/share/gugent/site/SetupOS
```

L'agent Linux exécute le script dans l'ordre spécifié par le répertoire d'éléments de travail et le nom du fichier de script.

Préparation du provisionnement SCCM

vRealize Automation démarre une machine provisionnée récemment à partir d'une image ISO, puis transmet le contrôle à la séquence des tâches SCCM spécifiée.

Le provisionnement SCCM est pris en charge pour le déploiement de systèmes d'exploitation Windows. Linux n'est pas pris en charge. La distribution et les mises à jour logicielles ne sont pas prises en charge.

La présentation de niveau supérieur de la procédure requise pour préparer le provisionnement SCCM est la suivante :

- 1 Consultez votre administrateur réseau pour vérifier que les conditions réseau requises sont satisfaites :
 - La communication avec SCCM nécessite le nom NetBios du serveur SCCM. Au moins un DEM doit être capable de restaurer le nom complet du serveur SCCM à son nom NetBios.
 - Le serveur SCCM et le serveur vRealize Automation doivent être sur le même réseau et disponibles l'un pour l'autre.
- 2 Créez un package logiciel incluant l'agent invité vRealize Automation. Reportez-vous à [Créer un package logiciel pour le provisionnement de SCCM](#).
- 3 Dans SCCM, créez la séquence des tâches souhaitée pour le provisionnement de la machine. La configuration finale doit consister en l'installation du package logiciel que vous avez créé contenant l'agent invité vRealize Automation. Pour plus d'informations sur la création de séquences des tâches et l'installation de packages logiciels, reportez-vous à la documentation SCCM.
- 4 Créez une image ISO avec démarrage en mode Zero Touch pour la séquence des tâches. Par défaut, SCCM crée une image ISO avec démarrage en mode Lite Touch. Pour plus d'informations sur la configuration de SCCM pour des images ISO de démarrage en mode Zero Touch, reportez-vous à la documentation SCCM.
- 5 Copiez l'image ISO à l'emplacement requis par votre plate-forme de virtualisation. Si vous ne le connaissez pas, reportez-vous à la documentation fournie par votre hyperviseur.
- 6 Réunissez les informations suivantes pour que les architectes du Blueprint puissent les inclure dans les Blueprints :
 - a Nom de la collection contenant la séquence des tâches.
 - b Nom de domaine complet du serveur SCCM sur lequel se situe la collection contenant la séquence.
 - c Code de site du serveur SCCM.
 - d Informations d'identification de niveau administrateur du serveur SCCM.
 - e (Facultatif) Pour les intégrations avec SCVMM, ISO, disque dur virtuel ou profil matériel à associer aux machines provisionnées.

Créer un package logiciel pour le provisionnement de SCCM

L'étape final de votre séquence de tâches SCCM doit être l'installation d'un package logiciel incluant l'agent invité vRealize Automation.

Procédure

- 1 Accédez à la page de la console de gestion du dispositif vRealize Automation.
Par exemple : `https://va-hostname.domain.com`.

- 2 Cliquez sur **Page des agents invités et logiciels** dans la section d'installation de composants vRealize Automation de la page.

Par exemple : `https://va-hostname.domain.com/software/index.html`.

La page **Programmes d'installation d'agents invités et logiciels** s'ouvre. Elle affiche des liens vers les téléchargements disponibles.

- 3 Cliquez sur les fichiers d'agents invités Windows (**32 bits**) ou (**64 bits**) dans la section d'installation de composants pour télécharger et enregistrer le fichier `GuestAgentInstaller.exe` ou `GuestAgentInstaller_x64.exe`.
- 4 Extrayez les fichiers de l'agent invité Windows vers un emplacement accessible à SCCM.
Cette opération affiche le répertoire `C:\VRMGuestAgent`. Ne renommez pas ce répertoire.
- 5 Créez un package logiciel à partir du fichier de définition `SCCMPackageDefinitionFile.sms`.
- 6 Mettez le package logiciel à disposition de votre point de distribution.
- 7 Sélectionnez le contenu des fichiers de l'agent invité Windows extraits comme étant vos fichiers sources.

Préparation du provisionnement de WIM

Provisionnez une machine en effectuant un démarrage dans un environnement WinPE, puis installez un système d'exploitation à l'aide de l'image WIM (Windows Imaging File) d'une machine de référence Windows.

Voici une présentation générale de la procédure requise pour préparer le provisionnement WIM :

- 1 Identifiez ou créez la zone de transfert. La zone de transfert doit être un répertoire de réseau qui peut être spécifié comme un chemin UNC ou monté comme un lecteur réseau par
 - La machine de référence.
 - Le système sur lequel vous créez l'image WinPE.
 - L'hôte de virtualisation où vous provisionnez les machines.
- 2 Assurez-vous que le réseau dispose d'un serveur DHCP. vRealize Automation ne peut pas provisionner de machines à l'aide d'une image WIM, sauf si DHCP est disponible.
- 3 Identifiez ou créez la machine de référence sur la plate-forme de virtualisation que vous prévoyez d'utiliser pour le provisionnement. Pour en savoir plus sur les conditions requises de vRealize Automation, reportez-vous à [Configuration requise de la machine de référence pour le provisionnement WIM](#). Pour plus d'informations sur la création d'une machine de référence, reportez-vous à la documentation fournie par votre hyperviseur.
- 4 À l'aide de System Preparation Utility for Windows, préparez le système d'exploitation de la machine de référence pour le déploiement. Reportez-vous à [Conditions requises de SysPrep pour la machine de référence](#).
- 5 Créez l'image WIM de la machine de référence. N'incluez aucun espace dans le nom du fichier image WIM, sinon le provisionnement échouera.

6 Créez une image WinPE incluant l'agent invité vRealize Automation.

- (Facultatif) Créez des scripts personnalisés de votre choix pour personnaliser des machines provisionnées et placez-les dans le répertoire approprié des éléments de travail.
- Si vous utilisez VirtIO pour des interfaces réseau ou de stockage, vous devez vous assurer que les pilotes requis sont inclus dans votre image WinPE et votre image WIM. Reportez-vous à [Préparation du provisionnement WIM avec des pilotes VirtIO](#).

Lorsque vous créez l'image WinPE, vous devez insérer manuellement l'agent invité vRealize Automation. Reportez-vous à [Insérer manuellement l'agent invité dans une image WinPE](#).

7 Placez l'image WinPE dans l'emplacement requis par votre plate-forme de virtualisation. Si vous ne connaissez pas l'emplacement, reportez-vous à la documentation de l'hyperviseur.

8 Collectez les informations suivantes à inclure dans le Blueprint :

- a Nom et emplacement de l'image ISO WinPE.
- b Nom du fichier WIM, chemin UNC au fichier WIM et index utilisé pour extraire l'image souhaitée du fichier WIM.
- c Le nom d'utilisateur et le mot de passe sous lesquels mapper le chemin de l'image WIM à un lecteur réseau sur la machine provisionnée.
- d (Facultatif) Si vous ne souhaitez pas accepter la valeur par défaut, K, lettre du lecteur à laquelle le chemin de l'image WIM est mappée sur la machine provisionnée.
- e Pour les intégrations avec vCenter Server, la version du système d'exploitation invité de vCenter Server avec lequel vCenter Server doit créer la machine.
- f (Facultatif) Pour les intégrations avec SCVMM, ISO, disque dur virtuel ou profil matériel à associer aux machines provisionnées.

Remarque Vous pouvez créer un groupe de propriétés pour inclure toutes ces informations requises. L'utilisation d'un groupe de propriétés facilite l'inclusion réussie de toutes les informations dans les Blueprints.

1 [Configuration requise de la machine de référence pour le provisionnement WIM](#)

Le provisionnement WIM nécessite la création d'une image WIM à partir d'une machine de référence. La machine de référence doit avoir la configuration requise minimale pour que l'image WIM fonctionne lors du provisionnement dans vRealize Automation.

2 [Conditions requises de SysPrep pour la machine de référence](#)

Un fichier de réponse SysPrep contient plusieurs paramètres requis utilisés pour le provisionnement WIM.

3 [Préparation du provisionnement WIM avec des pilotes VirtIO](#)

Si vous utilisez VirtIO pour des interfaces réseau ou de stockage, vous devez vous assurer que les pilotes requis sont inclus dans votre image WinPE et votre image WIM. VirtIO offre généralement des meilleures performances lors d'un provisionnement avec KVM (RHEV).

4 Insérer manuellement l'agent invité dans une image WinPE

Vous devez insérer manuellement l'agent invité vRealize Automation dans votre image WinPE.

Configuration requise de la machine de référence pour le provisionnement WIM

Le provisionnement WIM nécessite la création d'une image WIM à partir d'une machine de référence. La machine de référence doit avoir la configuration requise minimale pour que l'image WIM fonctionne lors du provisionnement dans vRealize Automation.

La présentation de niveau supérieur de la procédure à suivre pour préparer une machine de référence est la suivante :

- 1 Si le système d'exploitation de votre machine de référence est Windows Server 2008 R2, Windows Server 2012, Windows 7 ou Windows 8, l'installation par défaut crée une petite partition sur le disque dur du système en plus de la partition principale. vRealize Automation ne prend pas en charge les images WIM créées sur ce type de machines de références à plusieurs partitions. Vous devez supprimer cette partition pendant le processus d'installation.
- 2 Installez NET 4.5 et le Windows Automated Installation Kit (AIK) pour Windows 7 (y compris WinPE 3.0) sur la machine de référence.
- 3 Si le système d'exploitation de la machine de référence est Windows Server 2003 ou Windows XP, réinitialisez le mot de passe de l'administrateur pour qu'il soit vide. (Il n'y a pas de mot de passe.)
- 4 (Facultatif) Si vous souhaitez activer l'intégration de XenDesktop, installez et configurez un agent Citrix Virtual Desktop Agent.
- 5 (Facultatif) Un agent WMI est requis pour collecter certaines données sur une machine Windows gérée par vRealize Automation, par exemple l'état Active Directory du propriétaire d'une machine. Pour garantir une gestion réussie de machines Windows, vous devez installer un agent WMI (en général, sur l'hôte Manager Service) et activez l'agent pour qu'il collecte les données auprès des machines Windows. Reportez-vous à *Installation de vRealize Automation 7.3*.

Conditions requises de SysPrep pour la machine de référence

Un fichier de réponse SysPrep contient plusieurs paramètres requis utilisés pour le provisionnement WIM.

Tableau 1-15. paramètres SysPrep requis pour machine de référence Windows Server ou Windows XP

Paramètres GuiUnattended	Valeur
AutoLogon	Oui
AutoLogonCount	1

Tableau 1-15. paramètres SysPrep requis pour machine de référence Windows Server ou Windows XP (suite)

Paramètres GuiUnattended	Valeur
AutoLogonUsername	<i>username</i> (<i>nom d'utilisateur et mot de passe</i> sont les informations d'identification utilisées pour la connexion automatique lorsque la machine nouvellement provisionnée redémarre dans le système d'exploitation invité. L'administrateur est généralement utilisé.)
AutoLogonPassword	<i>mot de passe</i> correspondant au AutoLogonUsername.

Tableau 1-16. Paramètres SysPrep requis pour la machine de référence n'utilisant pas Windows Server 2003 ou Windows XP :

Paramètres AutoLogon	Valeur
Enabled	Oui
LogonCount	1
Username	<i>username</i> (<i>nom d'utilisateur et mot de passe</i> sont les informations d'identification utilisées pour la connexion automatique lorsque la machine nouvellement provisionnée redémarre dans le système d'exploitation invité. L'administrateur est généralement utilisé.)
Password	<i>password</i> (<i>nom d'utilisateur et mot de passe</i> sont les informations d'identification utilisées pour la connexion automatique lorsque la machine nouvellement provisionnée redémarre dans le système d'exploitation invité. L'administrateur est généralement utilisé.)
Remarque Pour les machines de référence utilisant une plateforme Windows ultérieure à Windows Server 2003/Windows XP, il vous faut définir le mot de passe de connexion automatique au moyen de la propriété personnalisée Sysprep.GuiUnattended.AdminPassword. Une méthode pratique pour garantir cela est de créer un groupe de propriétés qui comprend cette propriété personnalisée afin que les administrateurs de locataire et les gestionnaires de groupe d'activité puissent inclure ces informations correctement dans leurs Blueprints.	

Préparation du provisionnement WIM avec des pilotes VirtIO

Si vous utilisez VirtIO pour des interfaces réseau ou de stockage, vous devez vous assurer que les pilotes requis sont inclus dans votre image WinPE et votre image WIM. VirtIO offre généralement des meilleures performances lors d'un provisionnement avec KVM (RHEV).

Les pilotes Windows pour VirtIO sont inclus dans le cadre de Red Hat Enterprise Virtualization et sont situés dans le répertoire `/usr/share/virtio-win` du système de fichiers du gestionnaire Red Hat Enterprise Virtualization. Les pilotes sont également inclus dans les outils invités de Red Hat Enterprise Virtualization situés dans `/usr/share/rhev-guest-tools-iso/rhev-tools-setup.iso`.

Le processus de niveau supérieur permettant le provisionnement basé sur WIM avec des pilotes VirtIO est le suivant :

- 1 Créez une image WIM à partir d'une machine de référence Windows avec les pilotes VirtIO installés ou insérez les pilotes dans une image WIM existante.
- 2 Copiez les fichiers de pilotes VirtIO et insérez les pilotes dans une image WinPE.
- 3 Téléchargez l'ISO de l'image WinPE dans les domaines de stockage ISO de Red Hat Enterprise Virtualization à l'aide de la commande `rhev-iso-uploader`. Pour plus d'informations sur la gestion des images ISO dans RHEV, reportez-vous à la documentation Red Hat.
- 4 Créez un Blueprint KVM (RHEV) pour le provisionnement WIM et sélectionnez l'option ISO WinPE. La propriété personnalisée `VirtualMachine.Admin.DiskInterfaceType` doit être incluse à la valeur **VirtIO**. Un administrateur Fabric peut inclure ces informations dans un groupe de propriétés afin qu'elles soient incluses dans des Blueprints.

Les propriétés personnalisées `Image.ISO.Location` et `Image.ISO.Name` ne sont pas utilisées pour des Blueprints KVM (RHEV).

Insérer manuellement l'agent invité dans une image WinPE

Vous devez insérer manuellement l'agent invité vRealize Automation dans votre image WinPE.

Prérequis

- Sélectionnez un système Windows accessible depuis la zone de transit que vous avez préparé et sur lequel .NET 4.5 et le Kit d'installation personnalisée (Windows AIK) pour Windows 7 (incluant WinPE 3.0) sont installés.
- Créez un environnement WinPE.

Procédure

1 Installer l'agent invité dans une image WinPE

Vous devez copier manuellement les fichiers d'agent invité sur votre image WinPE.

2 Configurer le fichier `doagent.bat`

Vous devez configurer manuellement le fichier `doagent.bat`.

3 Configurer le fichier `doagentc.bat`

Vous devez configurer manuellement le fichier `doagentc.bat`.

4 Configurer les fichiers de propriétés de l'agent invité

Vous devez configurer manuellement les fichiers de propriétés de l'agent invité.

Procédure

- 1 [Installer l'agent invité dans une image WinPE.](#)
- 2 [Configurer le fichier doagent.bat.](#)
- 3 [Configurer le fichier doagentc.bat.](#)
- 4 [Configurer les fichiers de propriétés de l'agent invité.](#)

Installer l'agent invité dans une image WinPE

Vous devez copier manuellement les fichiers d'agent invité sur votre image WinPE.

Prérequis

- Sélectionnez un système Windows accessible depuis la zone de transit que vous avez préparé et sur lequel .NET 4.5 et le Kit d'installation personnalisée (Windows AIK) pour Windows 7 (incluant WinPE 3.0) sont installés.
- Créez un environnement WinPE.

Procédure

- ◆ Téléchargez et installez l'agent invité vRealize Automation depuis https://vRealize_VA_Hostname_fqdn/software/index.html.
 - a Téléchargez la version GuestAgentInstaller_ sur le lecteur C sur la machine de référence.
Sélectionnez le fichier GuestAgentInstaller.exe (32 bits) ou GuestAgentInstaller_x64.exe (64 bits) en fonction des spécifications de votre système d'exploitation.
 - b Cliquez avec le bouton droit de la souris et sélectionnez **Propriétés**.
 - c Cliquez sur **Général**.
 - d Cliquez sur **Débloquer**.
 - e Extrayez les fichiers dans
Cette opération affiche le répertoire C:\VRMGuestAgent. Ne renommez pas ce répertoire.

Suivant

[Configurer le fichier doagent.bat.](#)

Configurer le fichier doagent.bat

Vous devez configurer manuellement le fichier doagent.bat.

Prérequis

[Installer l'agent invité dans une image WinPE.](#)

Procédure

- 1 Accédez au répertoire VRMGuestAgent dans votre image WinPE.
Par exemple : C:\Program Files (x86)\VMware\Plugins\VRM Agent\VRMGuestAgent.
- 2 Effectuez une copie du fichier doagent-template.bat et nommez-le doagent.bat.
- 3 Ouvrez doagent.bat dans un éditeur de texte.
- 4 Remplacez toutes les instances de la chaîne #Dcac Hostname# par le nom de domaine complet et le numéro de l'hôte IaaS Manager Service.

Option	Description
Si vous utilisez un équilibrage de charge	Entrez le nom de domaine complet et le port de l'équilibrage de charge de IaaS Manager Service. Par exemple, manager_service_LB.mycompany.com:443
Sans équilibrage de charge	Entrez le nom de domaine complet et le port de la machine sur laquelle IaaS Manager Service est installé. Par exemple, manager_service.mycompany.com:443

- 5 Remplacez toutes les instances de la chaîne #Protocol# par la chaîne /ssl.
- 6 Remplacez toutes les instances de la chaîne #Comment# par REM (REM doit être suivi d'un espace de fin).
- 7 (Facultatif) Si vous utilisez des certificats auto-signés, supprimez le commentaire concernant la commande openssl.

```
echo QUIT | c:\VRMGuestAgent\bin\openssl s_client -connect
```

- 8 Enregistrez et fermez le fichier.
- 9 Modifiez le script Startnet.cmd de votre WinPE pour inclure le fichier doagent.bat en tant que script personnalisé.

Suivant

[Configurer le fichier doagentc.bat.](#)

Configurer le fichier doagentc.bat

Vous devez configurer manuellement le fichier doagentc.bat.

Prérequis

[Configurer le fichier doagent.bat.](#)

Procédure

- 1 Accédez au répertoire VRMGuestAgent dans votre image WinPE.
Par exemple : C:\Program Files (x86)\VMware\Plugins\VRM Agent\VRMGuestAgent.

- 2 Effectuez une copie du fichier `doagentsvc-template.bat` et nommez-le `doagentc.bat`.
- 3 Ouvrez `doagentc.bat` dans un éditeur de texte.
- 4 Supprimez toutes les instances de la chaîne `#Comment#`
- 5 Remplacez toutes les instances de la chaîne `#Dcac Hostname#` par le nom de domaine complet et le numéro de l'hôte Manager Service.

Le port par défaut de Manager Service est 443.

Option	Description
Si vous utilisez un équilibrage de charge	Entrez le nom de domaine complet et le port de l'équilibrage de charge de Manager Service. Par exemple, <code>load_balancer_manager_service.mycompany.com:443</code>
Sans équilibrage de charge	Entrez le nom de domaine complet et le port de Manager Service. Par exemple, <code>manager_service.mycompany.com:443</code>

- 6 Remplacez toutes les instances de la chaîne `#errorlevel#` par le caractère 1.
- 7 Remplacez toutes les instances de la chaîne `#Protocol#` par la chaîne `/ssl`.
- 8 Enregistrez et fermez le fichier.

Suivant

[Configurer les fichiers de propriétés de l'agent invité.](#)

Configurer les fichiers de propriétés de l'agent invité

Vous devez configurer manuellement les fichiers de propriétés de l'agent invité.

Prérequis

[Configurer le fichier `doagentc.bat`.](#)

Procédure

- 1 Accédez au répertoire `VRMGuestAgent` dans votre image WinPE.
Par exemple : `C:\Program Files (x86)\VMware\Plugins\VRM Agent\VRMGuestAgent`.
- 2 Effectuez une copie du fichier `gugent.properties` et nommez-le `gugent.properties.template`.
- 3 Effectuez une copie du fichier `gugent.properties.template` et nommez-le `gugentc.properties`.
- 4 Ouvrez `gugent.properties` dans un éditeur de texte.
- 5 Remplacez toutes les instances de la chaîne `GuestAgent.log` par la chaîne `X:/VRMGuestAgent/GuestAgent.log`.
- 6 Enregistrez et fermez le fichier.
- 7 Ouvrez `gugentc.properties` dans un éditeur de texte.

- 8 Remplacez toutes les instances de la chaîne GuestAgent.log par la chaîne C:/VRMGuestAgent/GuestAgent.log.
- 9 Enregistrez et fermez le fichier.

Préparation du provisionnement de l'image de machine virtuelle

Avant de provisionner des instances avec OpenStack, vous devez avoir des images de machine virtuelle et des types configurés dans le fournisseur OpenStack.

Images de machines virtuelles

Vous pouvez sélectionner une image de machine virtuelle dans une liste des images disponibles lors de la création de Blueprints pour des ressources OpenStack.

Une image de machine virtuelle est un modèle contenant une configuration logicielle, notamment un système d'exploitation. Les images de machines virtuelles sont gérées par le fournisseur OpenStack et sont importées pendant la collecte de données.

Si une image utilisée dans un Blueprint est ensuite supprimée du fournisseur OpenStack, elle est également supprimée du Blueprint. Si toutes les images sont supprimées d'un Blueprint, celui-ci est désactivé et ne peut plus être utilisé pour des demandes de machines tant qu'il n'est pas modifié pour ajouter au moins une image.

Types OpenStack

Vous pouvez sélectionner un ou plusieurs types lors de la création de Blueprints OpenStack.

Les types OpenStack sont des modèles de matériel virtuel définissant les spécifications de ressources de la machine pour des instances provisionnées dans OpenStack. Les types sont gérés par le fournisseur OpenStack et sont importés pendant la collecte de données.

vRealize Automation prend en charge plusieurs types de serveur OpenStack. Pour les informations les plus récentes sur la prise en charge des types de serveur OpenStack, reportez-vous à *Matrice de prise en charge de vRealize Automation* à l'adresse <https://www.vmware.com/support/pubs/vcac-pubs.html>.

Préparation du provisionnement de l'image de la machine Amazon

Préparez les images de la machine Amazon et les types d'instances pour le provisionnement dans vRealize Automation.

Présentation des images de machines Amazon

Vous pouvez sélectionner une image de machine Amazon dans une liste d'images disponibles lorsque vous créez des Blueprints de machines Amazon.

Une image de machine Amazon est un modèle contenant une configuration logicielle, notamment un système d'exploitation. Les images de machine sont gérées par des comptes d'Amazon Web Services. vRealize Automation gère les types d'instances disponibles pour le provisionnement.

L'image de machine Amazon et le type d'instance doivent être disponibles dans une région Amazon. Tous les types d'instances ne sont pas disponibles dans toutes les régions.

Vous pouvez sélectionner une image de machine Amazon fournie par Amazon Web Services, une communauté d'utilisateurs ou le site AWS Marketplace. Vous pouvez également créer et, facultativement, partager vos propres images de machines Amazon. Une seule image de machine Amazon peut être utilisée pour lancer une ou plusieurs instances.

Les considérations suivantes s'appliquent aux images de machines Amazon des comptes d'Amazon Web Services depuis lesquels vous provisionnez des machines de cloud :

- Chaque Blueprint doit spécifier une image de machine Amazon.
Une image de machine Amazon privée est disponible pour un compte spécifique et toutes ses régions. Une image de machine Amazon publique est disponible pour tous les comptes, mais uniquement dans une région spécifique de chaque compte.
- À la création d'un Blueprint, l'image de machine Amazon spécifiée est sélectionnée dans les régions dont les données ont été collectées. Si plusieurs comptes d'Amazon Web Services sont disponibles, le gestionnaire de groupes d'activité doit disposer de droits d'accès à n'importe quelle image de machine Amazon privée. La région de l'image de machine Amazon et l'emplacement spécifié pour l'utilisateur restreignent la demande de provisionnement aux réservations correspondant à la région et à l'emplacement.
- Utilisez des réservations et des stratégies pour distribuer des images de machines Amazon dans vos comptes d'Amazon Web Services. Utilisez des stratégies visant à restreindre le provisionnement entre un Blueprint et un ensemble de réservations spécifique.
- vRealize Automation ne peut pas créer de comptes d'utilisateurs sur une machine de cloud. La première fois que le propriétaire d'une machine se connecte à une machine de cloud, il doit se connecter en tant qu'administrateur et ajouter ses informations d'identification d'utilisateur vRealize Automation ou bien un administrateur doit le faire pour lui. Il peut ensuite se connecter à l'aide de ses informations d'identification d'utilisateur vRealize Automation.

Si l'image de machine Amazon génère le mot de passe administrateur à chaque démarrage, la page Modifier l'enregistrement de la machine affiche le mot de passe. Dans le cas contraire, le mot de passe est accessible dans le compte d'Amazon Web Services. Vous pouvez configurer toutes les images de machines Amazon pour générer le mot de passe administrateur à chaque démarrage. Vous pouvez également fournir des informations sur le mot de passe administrateur aux utilisateurs de support technique qui provisionnent des machines pour le compte d'autres utilisateurs.

- Pour autoriser des demandes Microsoft Windows Management Instrumentation (WMI) à distance sur des machines cloud provisionnées dans des comptes d'Amazon Web Services, autorisez un agent Microsoft Windows Remote Management (WinRM) à collecter des données de machines Windows gérées par vRealize Automation. Reportez-vous à *Installation de vRealize Automation 7.3*.
- Une image de machine Amazon privée peut être consultée entre plusieurs locataires.

Pour obtenir des informations complémentaires, reportez-vous aux rubriques sur les AMI (*Amazon Machine Images, images de machines Amazon*) dans la documentation Amazon.

Présentation des types d'instances d'Amazon

Un architecte IaaS sélectionne un ou plusieurs types d'instances Amazon lors de la création de Blueprints Amazon EC2. Un administrateur IaaS peut ajouter ou supprimer des types d'instances, afin de contrôler les choix mis à la disposition des architectes.

Une instance d'Amazon EC2 est un serveur virtuel pouvant exécuter des applications dans Amazon Web Services. Les instances sont créées à partir d'une image de machine Amazon et en choisissant un type d'instance approprié.

Pour provisionner une machine dans un compte Amazon Web Services, un type d'instance est appliqué à l'image de machine Amazon spécifiée. Les types d'instances disponibles sont répertoriés lorsque les architectes créent le Blueprint Amazon EC2. Les architectes sélectionnent un ou plusieurs types d'instances qui deviennent des choix disponibles pour les utilisateurs lorsqu'ils demandent de provisionner une machine. Les types d'instances doivent être pris en charge dans la région désignée.

Pour obtenir des informations complémentaires, reportez-vous aux rubriques *Sélection de types d'instances* et *Détails de l'instance d'Amazon EC2* dans la documentation d'Amazon.

Ajouter un type d'instance Amazon

vRealize Automation fournit plusieurs types d'instances à utiliser avec les Blueprints Amazon. Un administrateur peut ajouter et supprimer plusieurs types d'instances.

Les types d'instances de la machine gérés par les administrateurs IaaS sont mis à disposition des architectes de Blueprint lorsqu'ils créent ou modifient un Blueprint Amazon. Les images et les types d'instances de la machine Amazon sont mis à disposition par le biais du produit Amazon Web Services.

Prérequis

Connectez-vous à la console de vRealize Automation en tant qu'**administrateur IaaS**.

Procédure

- 1 Cliquez sur **Infrastructure > Administration > Types d'instances**.
- 2 Cliquez sur **Nouveau**.
- 3 Ajoutez un nouveau type d'instance en spécifiant les paramètres à suivre.

Pour en savoir plus sur les types d'instances d'Amazon et les valeurs de paramètres que vous pouvez spécifier, reportez-vous à la documentation d'Amazon Web Services (AWS) dans *Types d'instances EC2 - Amazon Web Services (AWS)* sur le site Web aws.amazon.com/ec2 et *Types d'instances* sur le site Web docs.aws.amazon.com.

- Nom
- Nom de l'API
- Nom du type
- Nom des performances d'E/S
- CPU

- Mémoire (Go)
- Stockage (Go)
- Unités de calcul

4 Cliquez sur l'icône **Enregistrer** (✓).

Lorsque les architectes IaaS créeront des Blueprints Amazon Web Services, ils pourront utiliser les types d'instances personnalisées que vous avez créées.

Suivant

Ajoutez des ressources de calcul à partir de votre point de terminaison dans un groupe Fabric. Reportez-vous à [Créer un groupe Fabric](#).

Scénario : préparation de ressources vSphere pour le provisionnement de machines dans Rainpole

En tant qu'administrateur vSphere créant des modèles pour vRealize Automation, vous souhaitez utiliser vSphere Web Client pour préparer le clonage de machines CentOS dans vRealize Automation.



Vous souhaitez convertir une machine de référence CentOS existante en un modèle vSphere. Pour ce faire, vous pouvez créer avec les architectes Rainpole des Blueprints afin de cloner des machines CentOS dans vRealize Automation. Pour empêcher la survenue de conflits lors du déploiement de plusieurs machines virtuelles avec des paramètres identiques, vous souhaitez aussi créer une spécification de personnalisation générale. Avec les architectes, vous l'utiliserez afin de créer des Blueprints de clone pour les modèles Linux.

Procédure

1 Scénario : convertir votre machine de référence CentOS en un modèle pour Rainpole

À l'aide de vSphere Client, vous convertissez la machine de référence CentOS existante en un modèle vSphere afin que les architectes IaaS de vRealize Automation s'y réfèrent comme base de leurs Blueprints de clone.

2 Scénario : créer une spécification de personnalisation pour le clonage de machines Linux dans Rainpole

À l'aide de vSphere Client, vous créez une spécification de personnalisation standard que les architectes IaaS de vRealize Automation peuvent utiliser lorsqu'ils créent des Blueprints de clone pour des machines Linux.

Scénario : convertir votre machine de référence CentOS en un modèle pour Rainpole

À l'aide de vSphere Client, vous convertissez la machine de référence CentOS existante en un modèle vSphere afin que les architectes IaaS de vRealize Automation s'y réfèrent comme base de leurs Blueprints de clone.

Procédure

- 1 Connectez-vous à votre machine de référence en tant qu'utilisateur root et préparez la machine à la conversion.

- a Supprimez les règles de persistance udev.

```
/bin/rm -f /etc/udev/rules.d/70*
```

- b Activez les machines clonées à partir de ce modèle de sorte qu'elles disposent d'identifiants uniques.

```
/bin/sed -i '/^\(HWADDR\|UUID\)=/d'
/etc/sysconfig/network-scripts/ifcfg-eth0
```

- c Mettez la machine hors tension.

```
shutdown -h now
```

- 2 Connectez-vous à vSphere Web Client en tant qu'administrateur.
- 3 Cliquez sur l'onglet **Options VM**.
- 4 Cliquez avec le bouton droit sur la machine de référence et sélectionnez **Modifier les paramètres**.
- 5 Entrez **Rainpole_centos_63_x86** dans la zone de texte **Nom de VM**.
- 6 Même si votre machine de référence dispose d'un système d'exploitation invité CentOS, sélectionnez **Red Hat Enterprise Linux 6 (64 bits)** dans le menu déroulant **Versión du SE invité**.

Si vous sélectionnez CentOS, votre modèle et votre spécification de personnalisation peuvent ne pas fonctionner comme vous le souhaitez.
- 7 Cliquez avec le bouton droit sur la machine de référence **Rainpole_centos_63_x86** dans vSphere Web Client, puis sélectionnez **Modèle > Convertir en modèle**.

vCenter Server marque la machine de référence Rainpole_centos_63_x86 en tant que modèle et affiche la tâche dans le panneau Tâches récentes.

Suivant

Pour empêcher la survenue de conflits lors du déploiement de plusieurs machines virtuelles avec des paramètres identiques, vous créez une spécification de personnalisation générale. Avec les architectes Rainpole, vous l'utiliserez afin de créer des Blueprints de clone pour les modèles Linux.

Scénario : créer une spécification de personnalisation pour le clonage de machines Linux dans Rainpole

À l'aide de vSphere Client, vous créez une spécification de personnalisation standard que les architectes IaaS de vRealize Automation peuvent utiliser lorsqu'ils créent des Blueprints de clone pour des machines Linux.

Procédure

- 1 Sur la page d'accueil, cliquez sur **Gestionnaire de spécification de personnalisation** pour ouvrir l'assistant.
- 2 Cliquez sur l'icône **Nouveau**.
- 3 Précisez les propriétés.
 - a Sélectionnez **Linux** dans le menu déroulant **Système d'exploitation VM cible**.
 - b Dans la zone de texte **Nom de la spécification de personnalisation**, entrez **Linux**.
 - c Entrez **Clonage Linux Rainpole avec vRealize Automation** dans la zone de texte **Description**.
 - d Cliquez sur **Suivant**.
- 4 Définissez un nom d'un ordinateur.
 - a Sélectionnez **Utiliser le nom de la machine virtuelle**.
 - b Dans la zone de texte **Nom de domaine**, entrez le domaine dans lequel les machines clonées vont être provisionnées.

Par exemple, **rainpole.local**.
 - c Cliquez sur **Suivant**.
- 5 Configurez les paramètres du fuseau horaire.
- 6 Cliquez sur **Suivant**.
- 7 Sélectionnez **Utiliser les paramètres réseau standard pour le système d'exploitation invité, y compris l'activation de DHCP sur toutes les interfaces réseau**.
- 8 Pour entrer les dernières informations requises, suivez les invites qui s'affichent.
- 9 Dans la page **Prêt à terminer**, vérifiez vos sélections et cliquez sur **Terminer**.

Vous pouvez utiliser la spécification de personnalisation afin de créer des Blueprints pour le clonage de machines Linux.

Suivant

Connectez-vous à la console vRealize Automation comme l'administrateur de configuration que vous avez créé pendant l'installation et demandez les éléments de catalogue qui établissent rapidement votre validation technique.

Préparation du provisionnement Logiciel

Utilisez Logiciel pour déployer des applications et des intergiciels dans le cadre du provisionnement de vRealize Automation pour les machines vSphere, vCloud Director, vCloud Air et Amazon AWS.

Vous pouvez déployer Logiciel sur des machines si le Blueprint prend en charge Logiciel et à condition d'avoir installé l'agent invité et l'agent de démarrage logiciel sur les machines de référence avant de les convertir en modèles, en snapshots ou en images de machine Amazon.

Pour obtenir des informations connexes sur la spécification des ports lors de la préparation du provisionnement, reportez-vous à *Guide sur la configuration sécurisée* et à *Architecture de référence* sur la page [Informations sur VMware vRealize Automation](#).

Tableau 1-17. Méthodes de provisionnement prenant en charge Logiciel

Type de machine	Méthode de provisionnement	Préparation requise
vSphere	Cloner	Un Blueprint de clone provisionne une machine virtuelle complète et indépendante à partir d'un modèle de machine virtuelle vCenter Server. Pour que les modèles de clonage prennent en charge les composants Logiciel, installez l'agent invité et l'agent de démarrage logiciel sur la machine de référence lorsque vous préparez un modèle pour clonage. Reportez-vous à Liste de vérification pour la préparation du provisionnement par le clonage .
vSphere	Clone lié	Un Blueprint de clone lié provisionne une copie à optimisation d'espace d'une machine vSphere à partir d'un snapshot et à l'aide d'une chaîne de disques delta, afin de suivre les différences par rapport à la machine parent. Pour que les Blueprints de clone lié prennent en charge les composants Logiciel, installez l'agent invité et l'agent de démarrage logiciel sur la machine avant de prendre le snapshot. Si la machine de snapshot est clonée à partir d'un modèle qui prend en charge Logiciel, les agents requis sont déjà installés.
vCloud Director	Cloner	Un Blueprint de clone provisionne une machine virtuelle complète et indépendante à partir d'un modèle de machine virtuelle vCenter Server. Pour que les modèles de clonage prennent en charge les composants Logiciel, installez l'agent invité et l'agent de démarrage logiciel sur la machine de référence lorsque vous préparez un modèle pour clonage. Reportez-vous à Liste de vérification pour la préparation du provisionnement par le clonage .

Tableau 1-17. Méthodes de provisionnement prenant en charge Logiciel (suite)

Type de machine	Méthode de provisionnement	Préparation requise
vCloud Air	Cloner	Un Blueprint de clone provisionne une machine virtuelle complète et indépendante à partir d'un modèle de machine virtuelle vCenter Server. Pour que les modèles de clonage prennent en charge les composants Logiciel, installez l'agent invité et l'agent de démarrage logiciel sur la machine de référence lorsque vous préparez un modèle pour clonage. Reportez-vous à Liste de vérification pour la préparation du provisionnement par le clonage .
Amazon AWS	Image de la machine Amazon	<p>Une image de machine Amazon est un modèle contenant une configuration logicielle, notamment un système d'exploitation. Pour créer une image de machine Amazon qui prend en charge Logiciel, connectez-vous à une instance de Amazon AWS en cours d'exécution et qui utilise un volume EBS pour le périphérique racine. Installez l'agent invité et l'agent de démarrage logiciel sur la machine de référence, puis créez une image de machine Amazon à partir de l'instance. Pour obtenir des instructions sur la création d'images de machine Amazon (AMI, Amazon Machine Image) soutenues par EBS, reportez-vous à la documentation relative à Amazon AWS.</p> <p>Pour que l'agent invité et l'agent de démarrage logiciel Logiciel fonctionnent sur les machines provisionnées, vous devez configurer la connectivité entre le réseau et VPC.</p>

Préparation du provisionnement de machines avec Logiciel

Pour prendre en charge les composants Logiciel, commencez par installer l'agent invité et l'agent de démarrage Logiciel sur la machine de référence avant de procéder à la conversion en modèle de clonage, à la création d'une image de machine Amazon ou à la prise d'un snapshot.

Préparer une machine de référence Windows pour prendre en charge Logiciel

Vous utilisez un seul script pour installer l'environnement d'exécution Java, l'agent invité et l'agent de démarrage Logiciel sur une machine de référence Windows. Depuis la machine de référence, vous pouvez créer un modèle pour le clonage, un snapshot ou une image de machine Amazon qui prend en charge les composants Logiciel.

Logiciel prend en charge les scripts avec Windows CMD et PowerShell 2.0.

Important Le processus de démarrage ne doit pas être interrompu. Configurez la machine virtuelle de sorte que rien n'interrompe le processus de démarrage de la machine virtuelle avant d'atteindre l'invite de connexion. Par exemple, vérifiez qu'aucun processus ni aucun script n'invite l'utilisateur à intervenir au démarrage de la machine virtuelle.

Prérequis

- Identifiez ou créez une machine de référence.
- Établissez une confiance sécurisée entre la machine de référence et votre hôte IaaS Manager Service. Reportez-vous à [Configurer l'agent invité pour approuver un serveur](#).

- Sur la machine de référence, vérifiez que l'utilisateur Darwin dispose d'un accès Log on as a service.
- Si vous prévoyez d'accéder à distance à la machine pour le dépannage ou autres raisons, installez les Services Bureau à distance (RDS).
- Supprimez les artefacts de configuration réseau des fichiers de configuration réseau.

Procédure

- 1 Connectez-vous au serveur de référence Windows en tant qu'administrateur.
- 2 Ouvrez un navigateur dans la page de téléchargement de logiciel sur le dispositif vRealize Automation.

`https://vrealize-automation-appliance-FQDN/software`
- 3 Enregistrez le fichier ZIP du modèle sur le serveur Windows.

`prepare_vra_template_windows.zip`
- 4 Extrayez le contenu ZIP dans un dossier et exécutez le script `prepare_vra_template.ps1` à l'aide d'une des commandes suivantes.
 - `PowerShell -NoProfile -ExecutionPolicy Bypass -Command .\prepare_vra_template.ps1`
 - `.\prepare_vra_template.bat`
- 5 Suivez les invites.
- 6 Lorsque vous avez terminé, arrêtez la machine virtuelle Windows.

Le script supprime tout invité précédent ou les agents de démarrage de Logiciel et installe les versions prises en charge de l'environnement d'exécution Java, de l'agent invité et de l'agent de démarrage de Logiciel.

Suivant

Convertissez la machine de référence en un modèle pour le clonage, un snapshot ou une image de machine Amazon. Chacun prend en charge les composants Logiciel et les architectes d'infrastructure peuvent les utiliser lors de la création de Blueprints.

Préparer une machine de référence Linux pour prendre en charge Logiciel

Vous utilisez un seul script pour installer l'environnement d'exécution Java, l'agent invité et l'agent de démarrage Logiciel sur votre machine de référence Linux. Depuis la machine de référence, vous pouvez créer un modèle pour le clonage, un snapshot ou une image de machine Amazon qui prend en charge les composants Logiciel.

Logiciel prend en charge l'exécution des scripts avec Bash.

Important Le processus de démarrage ne doit pas être interrompu. Configurez la machine virtuelle de sorte que rien n'interrompe le processus de démarrage de la machine virtuelle avant d'atteindre l'invite de connexion. Par exemple, vérifiez qu'aucun processus ni aucun script n'invite l'utilisateur à intervenir au démarrage de la machine virtuelle.

Prérequis

- Identifiez ou créez une machine de référence Linux.
- Vérifiez que les commandes suivantes sont disponibles, en fonction de votre système Linux :
 - yum ou apt-get
 - wget ou curl
 - python
 - dmidecode selon les exigences des fournisseurs de cloud
 - Configuration générale requise, telle que sed, awk, perl, chkconfig, unzip et grep selon votre distribution Linux

Vous pouvez également utiliser un éditeur pour inspecter le script `prepare_vra_template.sh` téléchargé qui expose les commandes qu'il utilise.

- Si vous prévoyez d'accéder à distance à la machine à des fins de dépannage ou pour d'autres raisons, installez OpenSSH.
- Supprimez les artefacts de configuration réseau des fichiers de configuration réseau.

Procédure

- 1 Connectez-vous à votre machine de référence en tant qu'utilisateur racine.
- 2 Téléchargez le module tar.gz modèle à partir du dispositif vRealize Automation.

```
wget https://vrealize-automation-appliance-  
FQDN/software/download/prepare_vra_template.tar.gz
```

Si votre environnement utilise des certificats auto-signés, vous aurez peut-être besoin de l'option `--no-check-certificate`.

```
wget --no-check-certificate https://vrealize-automation-appliance-  
FQDN/software/download/prepare_vra_template.tar.gz
```

- 3 Décompressez le module.


```
tar -xvf prepare_vra_template.tar.gz
```
- 4 Dans la sortie untar, recherchez le script du programme d'installation et rendez-le exécutable.


```
chmod +x prepare_vra_template.sh
```

5 Exécutez le script du programme d'installation.

```
./prepare_vra_template.sh
```

Si vous avez besoin de plus d'informations sur les options non interactives et les valeurs attendues, consultez l'aide du script.

```
./prepare_vra_template.sh --help
```

6 Suivez les invites.

Une confirmation s'affiche lorsque l'installation réussit. Si des erreurs et des journaux s'affichent, résolvez les erreurs et relancez le script.

7 Lorsque vous avez terminé, arrêtez la machine virtuelle Linux.

Le script supprime tout invité précédent ou les agents de démarrage de Logiciel et installe les versions prises en charge de l'environnement d'exécution Java, de l'agent invité et de l'agent de démarrage de Logiciel.

Suivant

Sur votre hyperviseur ou fournisseur de cloud, transformez la machine de référence en un modèle pour le clonage, un snapshot ou une image de machine Amazon. Chacun prend en charge les composants Logiciel et les architectes d'infrastructure peuvent les utiliser lors de la création de Blueprints.

Mise à jour de modèles de machines virtuelles existants dans vRealize Automation

Si vous mettez à jour vos modèles, des images de machine Amazon ou des snapshots pour la dernière version de l'agent de démarrage Windows de Logiciel ou si vous procédez à une mise à jour manuelle vers l'agent de démarrage Linux de Logicielle plus récent au lieu d'utiliser le script `prepare_vra_template.sh`, il vous faut supprimer toute version existante et tous les journaux.

Linux

Pour les machines de référence Linux, exécutez le script `prepare_vra_template.sh` réinitialise l'agent et supprime tous les journaux pour vous avant la réinstallation. Toutefois, si vous avez l'intention d'effectuer une installation manuelle, vous devez vous connecter à la machine de référence en tant qu'utilisateur racine et exécuter la commande pour réinitialiser et supprimer tous les artefacts.

```
/opt/vmware-appdirector/agent-bootstrap/agent_reset.sh
```

Windows

Pour les machines de référence Windows, il vous faut supprimer l'agent de démarrage Logiciel et l'agent invité vRealize Automation 6.0 ou ultérieur, ainsi que supprimer tout fichier de journal d'exécution. Dans une fenêtre de commande PowerShell, exécutez les commandes pour supprimer l'agent et les artefacts.

```
c:\opt\vmware-appdirector\agent-bootstrap\agent_bootstrap_removal.bat
c:\opt\vmware-appdirector\agent-bootstrap\agent_reset.bat
```

Scénario : préparer un modèle vSphere CentOS pour les Blueprints de la machine clonée et du composant logiciel

En tant qu'administrateur vCenter Server, vous voudrez préparer un modèle vSphere que vos architectes vRealize Automation peuvent utiliser pour cloner des machines CentOS Linux. Afin de vous assurer que votre modèle prend en charge les Blueprints avec composant logiciels, installez l'agent invité et l'agent de démarrage avant de créer un modèle à partir de votre machine de référence.

Prérequis

- Identifiez ou créez une machine de référence Linux CentOS sur laquelle VMware Tools est installé. Pensez à inclure au moins un adaptateur réseau pour fournir une connexion Internet au cas où les architectes de Blueprint n'ajoutent pas cette fonctionnalité au niveau du Blueprint. Pour plus d'informations sur la création de machines virtuelles, reportez-vous à la documentation de vSphere.
- Vous devez être connecté à vCenter Server pour convertir une machine virtuelle en un modèle. Vous ne pouvez pas créer de modèles si vous connectez vSphere directement à un hôte vSphere ESXi.

Procédure

1 Scénario : Préparer votre machine de référence pour des personnalisations d'agent invité et des composants logiciels

Si vous voulez que votre modèle puisse prendre en charge des composants logiciels, vous devez installer l'agent de démarrage logiciel et sa condition préalable, à savoir l'agent invité, sur votre machine de référence. Ces agents garantissent que les architectes de vRealize Automation qui utilisent votre modèle pourront inclure des composants logiciels dans leurs Blueprints.

2 Scénario : Convertir votre machine de référence CentOS en un modèle

Après avoir installé l'agent invité et l'agent de démarrage logiciel sur la machine de référence, convertissez cette dernière en un modèle que les architectes vRealize Automation peuvent utiliser pour créer des Blueprints de machine de clone.

3 Scénario : créer une spécification de personnalisation pour le clonage vSphere

Créez une spécification de personnalisation que vos architectes de Blueprint pourront utiliser avec votre modèle `cpb_centos_63_x84`.

Vous avez créé un modèle et une spécification de personnalisation à partir de votre machine de référence que les architectes de Blueprint peuvent utiliser pour créer des Blueprints vRealize Automation qui clonent des machines CentOS Linux. Comme vous avez installé l'agent de démarrage Logiciel et l'agent invité sur votre machine de référence, les architectes peuvent utiliser votre modèle pour créer des Blueprints d'élément de catalogue élaborés qui comprennent des composants Logiciel ou d'autres personnalisations d'agent invité telles que des exécutions de scripts ou des formatage de disques. Comme vous avez installé VMware Tools, les architectes et les administrateurs de catalogue peuvent autoriser les utilisateurs à réaliser des actions contre des machines telles que des reconfigurations, des snapshots ou des redémarrages.

Suivant

Une fois les utilisateurs, les groupes et les ressources de vRealize Automation configurés, vous pouvez utiliser votre modèle et votre spécification de personnalisation pour créer un Blueprint de machine pour le clonage. Reportez-vous à *Installation et configuration de vRealize Automation pour le scénario Rainpole*.

Scénario : Préparer votre machine de référence pour des personnalisations d'agent invité et des composants logiciels

Si vous voulez que votre modèle puisse prendre en charge des composants logiciels, vous devez installer l'agent de démarrage logiciel et sa condition préalable, à savoir l'agent invité, sur votre machine de référence. Ces agents garantissent que les architectes de vRealize Automation qui utilisent votre modèle pourront inclure des composants logiciels dans leurs Blueprints.

Pour simplifier le processus, téléchargez et exécutez un script vRealize Automation qui installe les deux agents au lieu de télécharger et d'installer des modules distincts.

Le script se connecte également à votre instance de Manager Service et télécharge le certificat SSL afin d'établir une connexion fiable entre Manager Service et les machines déployées à partir de votre modèle. Notez que laisser le script télécharger le certificat est une méthode moins sûre que de récupérer et d'installer manuellement le certificat SSL de Manager Service sur votre machine de référence dans `/usr/share/gugent/cert.pem`.

Procédure

- 1 Dans votre navigateur Web, ouvrez l'URL suivante :
`https://vrealize-automation-appliance-FQDN/software/index.html`
- 2 Enregistrez le script `prepare_vra_template.sh` sur votre machine de référence.
- 3 Sur la machine de référence, rendez `prepare_vra_template.sh` exécutable.

```
chmod +x prepare_vra_template.sh
```

- 4 Exécutez `prepare_vra_template.sh`.

```
./prepare_vra_template.sh
```

- 5 Suivez les invites.

Si vous avez besoin d'informations non interactives sur les options et les valeurs, entrez `./prepare_vra_template.sh --help`.

Un message de confirmation s'affiche une fois l'installation terminée. Si des erreurs et messages du journal s'affichent, corrigez les problèmes et exécutez à nouveau le script.

Scénario : Convertir votre machine de référence CentOS en un modèle

Après avoir installé l'agent invité et l'agent de démarrage logiciel sur la machine de référence, convertissez cette dernière en un modèle que les architectes vRealize Automation peuvent utiliser pour créer des Blueprints de machine de clone.

Après avoir converti votre machine de référence en modèle, vous ne pouvez pas modifier ou mettre sous tension le modèle à moins que vous le convertissiez de nouveau en une machine virtuelle.

Procédure

- 1 Connectez-vous à votre machine de référence en tant qu'utilisateur root et préparez la machine à la conversion.

- a Supprimez les règles de persistance udev.

```
/bin/rm -f /etc/udev/rules.d/70*
```

- b Activez les machines clonées à partir de ce modèle de sorte qu'elles disposent d'identifiants uniques.

```
/bin/sed -i '/^\(HWADDR\|UUID\)=/d'
/etc/sysconfig/network-scripts/ifcfg-eth0
```

- c Si vous avez redémarré ou reconfiguré la machine de référence après avoir installé l'agent d'amorce logicielle, réinitialisez l'agent.

```
/opt/vmware-appdirector/agent-bootstrap/agent_reset.sh
```

- d Mettez la machine hors tension.

```
shutdown -h now
```

- 2 Connectez-vous à vSphere Web Client en tant qu'administrateur.
- 3 Cliquez avec le bouton droit sur la machine de référence et sélectionnez **Modifier les paramètres**.
- 4 Dans la zone de texte **Nom de VM**, entrez **cpb_centos_63_x84**.
- 5 Même si votre machine de référence dispose d'un système d'exploitation invité CentOS, sélectionnez **Red Hat Enterprise Linux 6 (64 bits)** dans le menu déroulant **Version du SE invité**.

Si vous sélectionnez CentOS, votre modèle et votre spécification de personnalisation peuvent ne pas fonctionner comme vous le souhaitez.

- 6 Cliquez avec le bouton droit sur votre machine de référence dans vSphere Web Client et sélectionnez **Modèle > Convertir en modèle**.

vCenter Server marque la machine de référence `cpb_centos_63_x84` en tant que modèle et affiche la tâche dans le panneau Tâches récentes. Si vous avez déjà placé votre environnement vSphere dans la gestion de vRealize Automation, votre modèle est découvert pendant la prochaine collecte de données. Si vous n'avez pas encore configuré votre vRealize Automation, le modèle est collecté pendant ce processus.

Scénario : créer une spécification de personnalisation pour le clonage vSphere

Créez une spécification de personnalisation que vos architectes de Blueprint pourront utiliser avec votre modèle `cpb_centos_63_x84`.

Procédure

- 1 Connectez-vous à vSphere Web Client en tant qu'administrateur.
- 2 Sur la page d'accueil, cliquez sur **Gestionnaire de spécification de personnalisation** pour ouvrir l'assistant.
- 3 Cliquez sur l'icône **Nouveau**.
- 4 Cliquez sur l'icône **Nouveau**.
- 5 Précisez les propriétés.
 - a Sélectionnez **Linux** dans le menu déroulant **Système d'exploitation VM cible**.
 - b Entrez **Customspecs** dans la zone de texte **Nom de la spécification de personnalisation**.
 - c Entrez **Clonage cpb_centos_63_x84 avec vRealize Automation** dans la zone de texte **Description**.
 - d Cliquez sur **Suivant**.
- 6 Définissez un nom d'un ordinateur.
 - a Sélectionnez **Utiliser le nom de la machine virtuelle**.
 - b Dans la zone de texte **Nom de domaine**, entrez le domaine dans lequel les machines clonées vont être provisionnées.
 - c Cliquez sur **Suivant**.
- 7 Configurez les paramètres du fuseau horaire.
- 8 Cliquez sur **Suivant**.
- 9 Sélectionnez **Utiliser les paramètres réseau standard pour le système d'exploitation invité, y compris l'activation de DHCP sur toutes les interfaces réseau**.

Les administrateurs Fabric et les architectes d'infrastructure gèrent les paramètres réseau de la machine provisionnée avec des profils réseau qu'ils ont créés et qu'ils utilisent dans vRealize Automation.
- 10 Pour entrer les dernières informations requises, suivez les invites qui s'affichent.

11 Dans la page **Prêt à terminer**, vérifiez vos sélections et cliquez sur **Terminer**.

Scénario : Préparer l'importation du Blueprint de l'exemple d'application Dukes Bank pour vSphere

En tant qu'administrateur vCenter Server, vous voulez préparer un modèle Linux CentOS 6.x vSphere et une spécification de personnalisation que vous pouvez utiliser pour provisionner l'exemple d'application Dukes Bank vRealize Automation.

Vous souhaitez vous assurer que votre modèle prend en charge les composants logiciels de l'échantillon d'application. Vous installez donc l'agent invité et l'agent d'amorce logicielle sur votre machine de référence Linux avant de la convertir en un modèle et de créer une spécification de personnalisation. Vous désactivez SELinux sur votre machine de référence pour vous assurer que votre modèle prend en charge la mise en œuvre spécifique de MySQL utilisée dans l'exemple d'application Dukes Bank.

Prérequis

- Installez et configurez entièrement vRealize Automation. Reportez-vous à *Installation et configuration de vRealize Automation pour le scénario Rainpole*.
- Identifiez ou créez une machine de référence Linux CentOS 6.x sur laquelle VMware Tools est installé. Pour plus d'informations sur la création de machines virtuelles, reportez-vous à la documentation de vSphere.
- Vous devez être connecté à vCenter Server pour convertir une machine virtuelle en un modèle. Vous ne pouvez pas créer de modèles si vous connectez vSphere directement à un hôte vSphere ESXi.

Procédure

1 [Scénario : Préparer votre machine de référence pour l'exemple d'application vSphere Dukes Bank](#)

Vous souhaitez que votre modèle prenne en charge l'échantillon d'application Dukes Bank. Vous devez donc installer l'agent invité et l'agent d'amorce logicielle sur votre machine de référence afin que vRealize Automation puisse provisionner les composants logiciels. Pour simplifier le processus, vous téléchargez et exécutez un script vRealize Automation permettant d'installer l'agent invité et l'agent d'amorce logicielle au lieu de télécharger et d'installer les packages séparément.

2 [Scénario : Convertir votre machine de référence en un modèle pour l'application vSphere Dukes Bank](#)

Après avoir installé l'agent invité et l'agent de démarrage logiciel sur votre machine de référence, vous désactivez SELinux pour vous assurer que votre modèle prend en charge la mise en œuvre spécifique de MySQL utilisée dans l'exemple d'application Dukes Bank. Vous transformez votre machine de référence en un modèle que vous pouvez utiliser pour provisionner l'exemple d'application vSphere Dukes Bank.

3 [Scénario : Créer une spécification de personnalisation pour le clonage des machines de l'exemple d'application vSphere Dukes Bank](#)

Vous créez une spécification de personnalisation à utiliser avec votre modèle de machine Dukes Bank.

Vous créez un modèle et une spécification à partir de votre machine de référence prenant en charge l'exemple d'application Dukes Bank vRealize Automation.

Scénario : Préparer votre machine de référence pour l'exemple d'application vSphere Dukes Bank

Vous souhaitez que votre modèle prenne en charge l'échantillon d'application Dukes Bank. Vous devez donc installer l'agent invité et l'agent d'amorce logicielle sur votre machine de référence afin que vRealize Automation puisse provisionner les composants logiciels. Pour simplifier le processus, vous téléchargez et exécutez un script vRealize Automation permettant d'installer l'agent invité et l'agent d'amorce logicielle au lieu de télécharger et d'installer les packages séparément.

Procédure

- 1 Connectez-vous à votre machine de référence en tant qu'utilisateur root.
- 2 Téléchargez le script d'installation de votre dispositif vRealize Automation.

```
wget https://vRealize_VA_Hostname_fqdn/software/download/prepare_vra_template.sh
```

Si votre environnement utilise des certificats autosignés, vous pouvez avoir besoin d'utiliser l'option `wget --no-check-certificate`. Par exemple :

```
wget --no-check-certificate  
https://vRealize_VA_Hostname_fqdn/software/download/prepare_vra_template.sh
```

- 3 Rendez exécutable le script `prepare_vra_template.sh`.

```
chmod +x prepare_vra_template.sh
```

- 4 Exécutez le script du programme d'installation `prepare_vra_template.sh`.

```
./prepare_vra_template.sh
```

Pour obtenir des informations sur les options non interactives et les valeurs attendues, vous pouvez exécuter la commande `./prepare_vra_template.sh --help`.

- 5 Suivez les invites pour terminer l'installation.

Un message de confirmation s'affiche lorsque l'installation est terminée. Si un message et des journaux d'erreur s'affichent sur la console, résolvez les erreurs et exécutez à nouveau le script du programme d'installation.

Vous avez installé l'agent d'amorce logicielle et sa condition préalable, l'agent invité, pour vous assurer que l'échantillon d'application Dukes Bank provisionne avec succès des composants logiciels. Le script s'est également connecté à votre instance de Manager Service et a téléchargé le certificat SSL afin d'établir une connexion fiable entre Manager Service et les machines déployées à partir de votre modèle. Cette approche est moins sécurisée que d'obtenir le certificat SSL de Manager Service et de l'installer sur votre machine de référence dans `/usr/share/gugent/cert.pem`. De plus vous pouvez remplacer manuellement ce certificat dès à présent, si la sécurité est primordiale.

Scénario : Convertir votre machine de référence en un modèle pour l'application vSphere Dukes Bank

Après avoir installé l'agent invité et l'agent de démarrage logiciel sur votre machine de référence, vous désactivez SELinux pour vous assurer que votre modèle prend en charge la mise en œuvre spécifique de MySQL utilisée dans l'exemple d'application Dukes Bank. Vous transformez votre machine de référence en un modèle que vous pouvez utiliser pour provisionner l'exemple d'application vSphere Dukes Bank.

Après avoir converti votre machine de référence en modèle, vous ne pouvez pas modifier ou mettre sous tension le modèle à moins que vous le convertissiez de nouveau en une machine virtuelle.

Procédure

- 1 Connectez-vous à votre machine de référence en tant qu'utilisateur root.

- a Modifiez votre fichier `/etc/selinux/config` pour désactiver SELinux.

```
SELINUX=disabled
```

Si vous ne désactivez pas SELinux, le composant logiciel MySQL de l'application Duke's Bank Sample risque de ne pas fonctionner comme prévu.

- b Supprimez les règles de persistance udev.

```
/bin/rm -f /etc/udev/rules.d/70*
```

- c Activez les machines clonées à partir de ce modèle de sorte qu'elles disposent d'identifiants uniques.

```
/bin/sed -i '/^\(HWADDR\|UUID\)=/d'
/etc/sysconfig/network-scripts/ifcfg-eth0
```

- d Si vous avez redémarré ou reconfiguré la machine de référence après avoir installé l'agent d'amorce logicielle, réinitialisez l'agent.

```
/opt/vmware-appdirector/agent-bootstrap/agent_reset.sh
```

- e Mettez la machine hors tension.

```
shutdown -h now
```

- 2 Connectez-vous à vSphere Web Client en tant qu'administrateur.
- 3 Cliquez avec le bouton droit sur la machine de référence et sélectionnez **Modifier les paramètres**.
- 4 Entrez **dukes_bank_template** dans la zone de texte **Nom de VM**.
- 5 Si votre machine de référence dispose d'un système d'exploitation invité CentOS, sélectionnez **Red Hat Enterprise Linux 6 (64 bits)** dans le menu déroulant **Version du SE invité**.

Si vous sélectionnez CentOS, votre modèle et votre spécification de personnalisation peuvent ne pas fonctionner comme vous le souhaitez.

- 6 Cliquez sur **OK**.
- 7 Cliquez avec le bouton droit sur votre machine de référence dans vSphere Web Client et sélectionnez **Modèle > Convertir en modèle**.

vCenter Server marque votre machine de référence dukes_bank_template comme modèle et affiche la tâche dans le panneau Tâches récentes. Si vous avez déjà placé votre environnement vSphere dans la gestion de vRealize Automation, votre modèle est découvert pendant la prochaine collecte de données. Si vous n'avez pas encore configuré votre vRealize Automation, le modèle est collecté pendant ce processus.

Scénario : Créer une spécification de personnalisation pour le clonage des machines de l'exemple d'application vSphere Dukes Bank

Vous créez une spécification de personnalisation à utiliser avec votre modèle de machine Dukes Bank.

Procédure

- 1 Connectez-vous à vSphere Web Client en tant qu'administrateur.
- 2 Sur la page d'accueil, cliquez sur **Gestionnaire de spécification de personnalisation** pour ouvrir l'assistant.
- 3 Cliquez sur l'icône **Nouveau**.
- 4 Précisez les propriétés.
 - a Sélectionnez **Linux** dans le menu déroulant **Système d'exploitation VM cible**.
 - b Entrez **Customspecs_sample** dans la zone de texte **Nom de la spécification de personnalisation**.
 - c Entrez **Dukes Bank customization spec** dans la zone de texte **Description**.
 - d Cliquez sur **Suivant**.
- 5 Définissez un nom d'un ordinateur.
 - a Sélectionnez **Utiliser le nom de la machine virtuelle**.
 - b Entrez le domaine sur lequel vous souhaitez provisionner l'exemple d'application Dukes Bank dans la zone de texte **Nom de domaine**.
 - c Cliquez sur **Suivant**.

- 6 Configurez les paramètres du fuseau horaire.
- 7 Cliquez sur **Suivant**.
- 8 Sélectionnez **Utiliser les paramètres réseau standard pour le système d'exploitation invité, y compris l'activation de DHCP sur toutes les interfaces réseau**.

Les administrateurs Fabric et les architectes d'infrastructure gèrent les paramètres réseau de la machine provisionnée avec des profils réseau qu'ils ont créés et qu'ils utilisent dans vRealize Automation.

- 9 Pour entrer les dernières informations requises, suivez les invites qui s'affichent.
- 10 Dans la page **Prêt à terminer**, vérifiez vos sélections et cliquez sur **Terminer**.

Vous créez un modèle et une spécification de personnalisation que vous utilisez pour provisionner l'exemple d'application Dukes Bank.

Suivant

- 1 Créez un profil réseau externe pour fournir une passerelle et une plage d'adresses IP. Reportez-vous à [Créer un profil de réseau externe au moyen d'un fournisseur IPAM tiers](#).
- 2 Mappez votre profil réseau externe à votre réservation vSphere. Reportez-vous à [Créer une réservation pour Hyper-V, KVM, SCVMM, vSphere ou XenServer](#). L'exemple d'application ne peut pas être provisionné correctement sans un profil réseau externe.
- 3 Importez l'exemple d'application Duke's Bank dans votre environnement. Reportez-vous à [Scénario : Importer l'exemple d'application Dukes Bank pour vSphere et le configurer pour votre environnement](#).

Préparations de ressources et de locataires pour le provisionnement de Blueprints

2

Vous pouvez configurer plusieurs environnements de locataires, chacun disposant de ses propres groupes d'utilisateurs et d'un accès unique aux ressources que vous placez sous la gestion de vRealize Automation.

Ce chapitre aborde les rubriques suivantes :

- [Configuration des paramètres de locataire](#)
- [Configuration des ressources](#)

Configuration des paramètres de locataire

Les administrateurs de locataires configurent les paramètres de locataires tels que l'authentification des utilisateurs. Ils gèrent également les rôles d'utilisateur et les groupes d'activité. Les administrateurs système et les administrateurs de locataires configurent des options, telles que les serveurs de messagerie afin de gérer les notifications, et la personnalisation de la console vRealize Automation.

Vous pouvez utiliser la liste de contrôle Configuration des paramètres de locataire afin d'afficher un aperçu de haut niveau de la séquence d'étapes requises pour configurer les paramètres de locataire.

Tableau 2-1. Liste de contrôle pour la configuration des paramètres de locataire

Tâche	Rôle vRealize Automation	Détails
<input type="checkbox"/> Créez des comptes d'utilisateurs locaux et désignez un administrateur de locataires.	Administrateur système	Pour obtenir un exemple de création de comptes d'utilisateurs locaux, reportez-vous à la section <i>Installation et configuration de vRealize Automation pour le scénario Rainpole</i> .
<input type="checkbox"/> Configurez la fonctionnalité Gestion des annuaires de façon à définir la gestion de l'identité des locataires et les paramètres de contrôle d'accès.	Administrateur de locataire	Choix des options de configuration de Directories Management
<input type="checkbox"/> Créez des groupes d'activité et des groupes personnalisés, puis octroyez des droits d'accès d'utilisateur à la console vRealize Automation.	Administrateur de locataire	Configuration de groupes et de rôles d'utilisateur

Tableau 2-1. Liste de contrôle pour la configuration des paramètres de locataire (suite)

Tâche	Rôle vRealize Automation	Détails
<input type="checkbox"/> (Facultatif) Créez des locataires supplémentaires afin que les utilisateurs puissent accéder aux applications appropriées et aux ressources dont ils ont besoin pour effectuer les tâches qui leur sont attribuées.	Administrateur système	Créer des locataires supplémentaires
<input type="checkbox"/> (Facultatif) Configurez la personnalisation de la connexion du locataire et des pages d'application de la console vRealize Automation.	<ul style="list-style-type: none"> ■ Administrateur système ■ Administrateur de locataire 	Configuration de la personnalisation
<input type="checkbox"/> (Facultatif) Configurez vRealize Automation pour que des notifications soient adressées aux utilisateurs lorsque des événements précis se produisent.	<ul style="list-style-type: none"> ■ Administrateur système ■ Administrateur de locataire 	Liste de contrôle de la configuration des notifications
<input type="checkbox"/> (Facultatif) Configurez vRealize Orchestrator de façon à prendre en charge XaaS et d'autres fichiers d'extensibilité.	<ul style="list-style-type: none"> ■ Administrateur système ■ Administrateur de locataire 	Configuration de vRealize Orchestrator
<input type="checkbox"/> (Facultatif) Créez un fichier de protocole de bureau à distance personnalisé que les architectes IaaS utilisent dans les Blueprints afin de configurer les paramètres RDP.	Administrateur système	Créer un fichier Remote Desktop Protocol (RDP) personnalisé pour prendre en charge les connexions RDP des machines provisionnées
<input type="checkbox"/> (Facultatif) Définissez les emplacements de centre de données que vos administrateurs d'infrastructure et architectes IaaS peuvent exploiter pour permettre aux utilisateurs de sélectionner un emplacement approprié pour le provisionnement lorsqu'ils demandent des machines.	Administrateur système	Pour voir un exemple d'ajout d'emplacements de centre de données, consultez la section Scénario : ajouter des emplacements de centre de données pour des déploiements inter-région .

Choix des options de configuration de Directories Management

Vous pouvez utiliser les fonctionnalités de Directories Management vRealize Automation afin de configurer un lien Active Directory conformément aux conditions requises pour l'authentification des utilisateurs.

Directories Management offre de nombreuses options de configuration afin de permettre une personnalisation poussée de l'authentification des utilisateurs.

Tableau 2-2. Choix des options de configuration de Directories Management

Option de configuration	Procédure
Configurer un lien vers votre produit Active Directory.	<ol style="list-style-type: none"> 1 Configurer un lien vers votre produit Active Directory. Reportez-vous à Configurer un lien Active Directory utilisant le protocole LDAP/IWA. 2 Si vous avez configuré vRealize Automation en vue de la haute disponibilité, consultez la section Configurer Directories Management pour High Availability.
(Facultatif) Améliorez la sécurité d'un lien Active Directory reposant sur un ID d'utilisateur et un mot de passe en configurant une intégration bidirectionnelle aux services fédérés Active Directory.	Configurer une relation de confiance bidirectionnelle entre vRealize Automation et Active Directory
(Facultatif) Ajoutez des utilisateurs et des groupes à un lien Active Directory existant.	Ajouter des utilisateurs ou des groupes à une connexion Active Directory .
(Facultatif) Modifiez la stratégie par défaut pour appliquer des règles personnalisées à un lien Active Directory.	Gérer la stratégie d'accès de l'utilisateur .
(Facultatif) Configurez les plages réseau pour restreindre les adresses IP par lesquelles les utilisateurs se connectent au système et gérez les restrictions de connexion (délai d'expiration, nombre de tentatives de connexion avant verrouillage).	Ajout ou modification d'une plage réseau .

Présentation de Directories Management

Les administrateurs de locataires peuvent configurer des paramètres de gestion et de contrôle d'accès d'identité de locataire à l'aide des options de la fonctionnalité Directories Management sur la console d'application de vRealize Automation.

Pour gérer les paramètres suivants, accédez à l'onglet **Administration > Directories Management**.

Tableau 2-3. Paramètres de Directories Management

Configuration	Description
Annuaire	<p>La page Annuaire permet de créer et de gérer des liens Active Directory pour la prise en charge des paramètres d'authentification et d'autorisation des utilisateurs locaux vRealize Automation. Vous devez créer un ou plusieurs annuaires, puis les synchroniser avec votre déploiement Active Directory. Cette page affiche le nombre de groupes et d'utilisateurs synchronisés à l'annuaire, ainsi que la dernière synchronisation. Pour démarrer manuellement la synchronisation d'annuaire, vous pouvez cliquer sur Synchroniser maintenant.</p> <p>Reportez-vous à Utilisation de la gestion des répertoires pour créer un lien Active Directory.</p> <p>Lorsque vous cliquez sur un annuaire, puis sur le bouton Paramètres de synchronisation, vous pouvez modifier les paramètres de synchronisation, accéder à la page Fournisseurs d'identité et afficher le journal de synchronisation.</p> <p>Sur la page des paramètres de synchronisation des annuaires, vous pouvez programmer la fréquence de synchronisation, voir la liste de domaines associés à cet annuaire, modifier la liste d'attributs mappés, mettre à jour la liste des utilisateurs et des groupes qui se synchronisent et définir les cibles de protection.</p>
Connecteurs	<p>La page Connecteurs répertorie les connecteurs déployés pour le réseau d'entreprise. Un connecteur synchronise les données des utilisateurs et des groupes entre Active Directory et le service Directories Management. Lorsque ce connecteur est utilisé comme fournisseur d'identité, il authentifie les utilisateurs auprès du service. Chaque dispositif vRealize Automation contient un connecteur par défaut. Reportez-vous à Gestion des connecteurs et des clusters de connecteurs.</p>
Attributs utilisateur	<p>La page Attributs utilisateur répertorie les attributs utilisateur par défaut qui sont synchronisés dans l'annuaire et vous pouvez ajouter d'autres attributs et les mapper aux attributs Active Directory. Reportez-vous à Sélection des attributs à synchroniser avec l'annuaire.</p>
Plages réseau	<p>Cette page répertorie les plages réseau configurées pour votre système. Vous pouvez configurer une plage réseau pour accorder un accès aux utilisateurs via ces adresses IP. Vous pouvez ajouter des plages réseau supplémentaires et modifier les plages existantes. Reportez-vous à Ajout ou modification d'une plage réseau.</p>
Fournisseurs d'identité	<p>La page Fournisseurs d'identité répertorie les fournisseurs disponibles dans le système. Le système vRealize Automation contient un connecteur qui sert de fournisseur d'identité par défaut et qui suffit à satisfaire les besoins de nombreux utilisateurs. Vous pouvez ajouter des instances de fournisseurs d'identité tiers ou avoir une combinaison des deux.</p> <p>Reportez-vous à Configurer une connexion de fournisseur d'identité tiers.</p>
Stratégies	<p>La page Stratégies répertorie la stratégie d'accès par défaut et toute autre stratégie d'accès aux applications Web que vous avez créées. Les stratégies sont un ensemble de règles qui spécifient les critères à satisfaire pour que les utilisateurs puissent accéder à leurs portails d'applications ou lancer des applications Web mises à leur disposition. La stratégie par défaut devrait convenir à la plupart des déploiements de vRealize Automation. Toutefois, vous pouvez la modifier selon vos besoins. Reportez-vous à Gérer la stratégie d'accès de l'utilisateur.</p>

Concepts fondamentaux liés à Active Directory

Plusieurs concepts liés à Active Directory sont indispensables à la compréhension du mode d'intégration de la fonctionnalité Directories Management à vos environnements Active Directory.

Connector

Le connector, composant du service, exécute les fonctions suivantes.

- Synchronise les données des utilisateurs et des groupes entre Active Directory et le service.

- Lorsqu'il est utilisé comme fournisseur d'identité, il authentifie les utilisateurs sur le service.

Le connector est le fournisseur d'identité par défaut. Pour les méthodes d'authentification que le connector prend en charge, consultez le guide *Administration de VMware Identity Manager*. Vous pouvez également utiliser les fournisseurs d'identité tiers prenant en charge le protocole SAML 2.0. Utilisez un fournisseur d'identité tiers pour un type d'authentification non pris en charge par le connector ou pour un type d'authentification pris en charge par le connector, si le fournisseur d'identité tiers est préférable en fonction de la stratégie de sécurité de votre entreprise.

Remarque Même si vous utilisez des fournisseurs d'identité tiers, vous devez configurer le connector pour synchroniser les données des utilisateurs et des groupes.

Annuaire

Le service Directories Management possède son propre concept d'annuaire, qui utilise les attributs et paramètres Active Directory pour définir les utilisateurs et les groupes. Vous devez créer un ou plusieurs annuaires, puis les synchroniser avec votre déploiement Active Directory. Vous pouvez créer les types d'annuaires suivants dans le service.

- Active Directory via LDAP : Créez ce type d'annuaire si vous prévoyez de vous connecter à un seul environnement de domaine Active Directory. Pour le type d'annuaire Active Directory via LDAP, le connector se lie à Active Directory via une authentification Bind simple.
- Active Directory, authentification Windows intégrée. Créez ce type d'annuaire si vous prévoyez de vous connecter à un environnement Active Directory à forêts et domaines multiples. Le connector se lie à Active Directory via l'authentification Windows intégrée.

Le type et le nombre d'annuaires que vous créez varie selon votre environnement Active Directory, par exemple à domaine simple ou multiple, et le type d'approbation utilisé entre les domaines. Dans la plupart des environnements, vous devez créer un seul annuaire.

Le service n'a pas accès direct à Active Directory. Seul le connector a accès direct à Active Directory. Par conséquent, vous devez associer chaque annuaire créé dans le service à une connector instance.

Travailleur

Lorsque vous associez un annuaire à une instance de connector, le connector crée une partition pour l'annuaire associé, appelée travailleur. Une instance de connector peut être associée à plusieurs travailleurs. Chaque travailleur fait office de fournisseur d'identité. Vous devez définir et configurer les méthodes d'authentification pour chaque travailleur.

Le connector synchronise les données des utilisateurs et des groupes entre Active Directory et le service au moyen d'un ou de plusieurs travailleurs.

La même instance de connector ne peut pas comporter deux travailleurs de type Authentification Windows intégrée.

Environnements Active Directory

Vous pouvez intégrer le service dans un environnement Active Directory composé d'un seul domaine Active Directory, de plusieurs domaines dans une forêt Active Directory unique, ou de plusieurs domaines dans différentes forêts Active Directory.

Environnement à un seul domaine Active Directory

Un déploiement Active Directory unique vous permet de synchroniser les utilisateurs et les groupes d'un seul domaine Active Directory.

Reportez-vous à [Configurer un lien Active Directory utilisant le protocole LDAP/IWA](#). Pour cet environnement, lorsque vous ajoutez un annuaire au service, sélectionnez l'option Active Directory via LDAP.

Environnement Active Directory à domaines multiples, forêt unique

Un déploiement à domaines multiples, forêt unique vous permet de synchroniser des utilisateurs et des groupes à partir de multiples domaines Active Directory au sein d'une forêt unique.

Vous pouvez configurer le service pour cet environnement Active Directory en tant qu'annuaire de type Authentification Windows intégrée à Active Directory unique ou en tant qu'annuaire de type Active Directory via LDAP configuré avec l'option de catalogue global.

- L'option recommandée consiste à créer un annuaire de type Authentification Windows intégrée à Active Directory unique.

Reportez-vous à [Configurer un lien Active Directory utilisant le protocole LDAP/IWA](#). Lorsque vous ajoutez un annuaire pour cet environnement, sélectionnez l'option Active Directory (Authentification Windows intégrée).

Environnement Active Directory à forêts multiples avec relations d'approbation

Un déploiement Active Directory à forêts multiples avec relations d'approbation vous permet de synchroniser des utilisateurs et des groupes provenant de plusieurs domaines Active Directory dans des forêts où des relations d'approbation bidirectionnelles existent entre les domaines.

Reportez-vous à [Configurer un lien Active Directory utilisant le protocole LDAP/IWA](#). Lorsque vous ajoutez un annuaire pour cet environnement, sélectionnez l'option Active Directory (Authentification Windows intégrée).

Environnement Active Directory à forêts multiples sans relations d'approbation

Un déploiement Active Directory à forêts multiples sans relations d'approbation vous permet de synchroniser des utilisateurs et des groupes provenant de plusieurs domaines Active Directory dans des forêts sans relation d'approbation entre les domaines. Dans cet environnement, vous devez créer plusieurs annuaires dans le service, à raison d'un annuaire par forêt.

Reportez-vous à [Configurer un lien Active Directory utilisant le protocole LDAP/IWA](#). Le type d'annuaire que vous créez dans le service varie selon la forêt. Pour les forêts à plusieurs domaines, sélectionnez l'option Active Directory (Authentification Windows intégrée). Pour une forêt ne comptant qu'un seul domaine, sélectionnez l'option Active Directory via LDAP.

Utilisation de la gestion des répertoires pour créer un lien Active Directory

Après avoir créé des locataires vRealize Automation, vous devez vous connecter à la console du système en tant qu'administrateur de locataire et créer un lien Active Directory afin de prendre en charge l'authentification de l'utilisateur.

Lorsque vous configurez une connexion Active Directory à l'aide de la fonction de gestion des répertoires, trois options de protocole de communication Active Directory sont disponibles.

- Active Directory sur LDAP : ce protocole prend en charge la recherche d'emplacement du service DNS par défaut.
- Active Directory (authentification Windows intégrée) : ce protocole vous permet de configurer le domaine à joindre. Le protocole Active Directory sur LDAP convient aux déploiements à domaine unique. Utilisez le protocole Active Directory (authentification Windows intégrée) pour tous les déploiements à domaines multiples et à forêts multiples.
- OpenLDAP : vous pouvez utiliser la version libre de LDAP pour prendre en charge l'authentification des utilisateurs de la fonction de gestion des répertoires.

Après avoir sélectionné un protocole de communication et configuré un lien Active Directory, vous pouvez spécifier les domaines à utiliser avec la configuration Active Directory, puis sélectionner les utilisateurs et les groupes à synchroniser avec la configuration spécifiée.

Configurer un lien Active Directory utilisant le protocole LDAP/IWA

Vous pouvez configurer un lien Active Directory utilisant le protocole LDAP/IWA pour accompagner l'authentification utilisateur avec la fonctionnalité Directories Management pour configurer un lien avec Active Directory permettant de prendre en charge l'authentification utilisateur pour tous les locataires et sélectionner des utilisateurs, et des groupes à synchroniser avec le répertoire Directories Management.

Pour plus d'informations et d'instructions concernant l'utilisation d'OpenLDAP avec Gestion des annuaires, reportez-vous à [Configurer une connexion à un annuaire OpenLDAP](#).

Pour Active Directory (authentification Windows intégrée), lorsque vous avez configuré un annuaire Active Directory à forêts multiples et que le groupe local du domaine contient des membres de domaines provenant de différentes forêts, assurez-vous que l'utilisateur Bind est ajouté au groupe Administrateurs du domaine dans lequel se trouve le groupe local du domaine. Si vous ne le faites pas, ces membres ne figureront pas dans le groupe local du domaine.

Prérequis

- Sélectionnez les attributs par défaut souhaités et ajoutez des attributs supplémentaires sur la page Attributs utilisateur. Reportez-vous à [Sélection des attributs à synchroniser avec l'annuaire](#).
- Liste des groupes et des utilisateurs Active Directory à synchroniser depuis Active Directory.
- Si Active Directory requiert un accès via SSL ou STARTTLS, le certificat d'autorité de certification racine du contrôleur de domaine Active Directory est requis.
- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

- 1 Sélectionnez **Administration > Gestion des répertoires > Répertoires**.
- 2 Cliquez sur **Ajouter un annuaire** et sélectionnez **Ajouter Active Directory via LDAP/IWA**.
- 3 Sur la page Ajouter un annuaire, spécifiez l'adresse IP du serveur Active Directory dans la zone de texte **Nom de l'annuaire**.
- 4 Sélectionnez le protocole de communication Active Directory approprié à l'aide des boutons radio situés sous la zone de texte **Nom de l'annuaire**.

Option	Description
Authentification Windows	Sélectionnez Active Directory (authentification Windows intégrée) . Pour l'authentification Windows intégrée à Active Directory, les informations requises incluent l'adresse et le mot de passe de l'UPN de l'utilisateur Bind du domaine.
LDAP	Sélectionnez Active Directory via LDAP . Pour Active Directory via LDAP, les informations requises incluent le nom unique de base, le nom unique de liaison et le mot de passe du nom unique de liaison.

- 5 Configurez le connecteur qui synchronise les utilisateurs entre Active Directory et l'annuaire VMware Directories Management dans la section Synchronisation d'annuaires et authentification.

Option	Description
Connecteur de synchronisation	Sélectionnez le connecteur approprié à utiliser avec votre système. Chaque dispositif vRealize Automation contient un connecteur par défaut. Consultez votre administrateur système si vous avez besoin d'aide pour choisir le connecteur approprié.
Authentification	<p>Cliquez sur le bouton radio approprié pour indiquer si le connecteur sélectionné effectue également l'authentification.</p> <p>Si vous utilisez Active Directory (authentification Windows intégrée), avec un fournisseur d'identité tiers pour authentifier les utilisateurs, cliquez sur Non. Après avoir configuré la connexion Active Directory pour synchroniser les utilisateurs et les groupes, utilisez la page Fournisseurs d'identité pour ajouter le fournisseur d'identité tiers à des fins d'authentification.</p> <p>Pour plus d'informations sur l'utilisation des adaptateurs d'authentification tels que PasswordpddAdapter, SecurlDAdapter et RadiusAuthAdapter, consultez le <i>Guide d'administration de VMware Identity Manager</i>.</p>
Attribut de recherche d'annuaire	<p>Sélectionnez l'attribut de compte approprié contenant le nom d'utilisateur. VMware recommande d'utiliser l'attribut sAMAccount plutôt que userPrincipalName. Si vous utilisez userPrincipalName pour les opérations de synchronisation, l'intégration à un logiciel secondaire et tiers qui requiert un nom d'utilisateur peut ne pas fonctionner correctement.</p> <p>Remarque Si vous sélectionnez sAMAccountName lors de l'utilisation d'un catalogue global, indiqué en cochant la case Cet annuaire comporte un catalogue Global dans la zone Emplacement du serveur, les utilisateurs ne pourront pas se connecter.</p>

- 6 Entrez les informations appropriées dans la zone de texte **Emplacement du serveur** si vous avez sélectionné **Active Directory via LDAP** ou renseignez les zones de texte **Détails du domaine de jonction** si vous avez sélectionné **Active Directory (authentification Windows intégrée)**.

Option	Description
Emplacement du serveur : s'affiche lorsque l'option Active Directory via LDAP est sélectionnée	<ul style="list-style-type: none"> ■ Si vous voulez utiliser l'emplacement du service DNS pour localiser les domaines Active Directory, laissez la case en regard de l'option Cet annuaire prend en charge l'emplacement du service DNS cochée. <p>Remarque Vous ne pouvez pas remplacer l'attribution du port par 636 si vous sélectionnez cette option.</p> <p>Un fichier <code>domain_krb.properties</code>, rempli automatiquement avec une liste de contrôleurs de domaine, est créé avec le répertoire. Reportez-vous à À propos de la sélection des contrôleurs de domaine.</p> <p>Si l'annuaire Active Directory nécessite le chiffrement STARTTLS, cochez la case Cet annuaire exige que toutes les connexions utilisent STARTTLS dans la section Certificats, puis copiez et collez le certificat d'autorité de certification racine Active Directory dans le champ Certificat SSL.</p> <ul style="list-style-type: none"> ■ Si l'annuaire Active Directory spécifié n'utilise pas la recherche d'emplacement du service DNS, désélectionnez la case en regard de l'option Cet annuaire prend en charge l'emplacement du service DNS dans le champ Emplacement du serveur et entrez le nom d'hôte et le numéro de port du serveur Active Directory dans les zones de texte appropriées. <p>Cochez la case Cet annuaire comporte un catalogue Global si l'instance d'Active Directory associée utilise un catalogue global. Un catalogue global contient une représentation de tous les objets dans chaque domaine de la forêt Active Directory multi-domaines.</p> <p>Pour configurer l'annuaire comme catalogue global, reportez-vous à la section Environnement Active Directory à forêt unique et domaines multiples au chapitre Environnements Active Directory.</p> <p>Si Active Directory requiert un accès via SSL, cochez la case en regard de l'option Cet annuaire exige que toutes les connexions se fassent par SSL sous l'en-tête Certificats, puis fournissez le certificat SSL d'Active Directory.</p> <p>Lorsque vous sélectionnez cette option, le port 636 est utilisé automatiquement et ne peut pas être modifié.</p> <p>Vérifiez que le certificat est au format PEM et inclut les lignes BEGIN CERTIFICATE et END CERTIFICATE.</p>
Détails du domaine de jonction - S'affiche lorsqu'Active Directory (authentification Windows intégrée) est sélectionné	<p>Entrez les informations d'identification appropriées dans les zones de texte Nom de domaine, Nom de l'utilisateur administrateur de domaine et Mot de passe de l'administrateur de domaine.</p> <p>Si l'annuaire Active Directory nécessite le chiffrement STARTTLS, cochez la case Cet annuaire exige que toutes les connexions utilisent STARTTLS dans la section Certificats, puis copiez et collez le certificat d'autorité de certification racine Active Directory dans le champ Certificat SSL.</p> <p>Vérifiez que le certificat est au format PEM et inclut les lignes BEGIN CERTIFICATE et END CERTIFICATE.</p>

Option	Description
	Si l'annuaire utilise plusieurs domaines, ajoutez les certificats d'autorité de certification racine pour tous les domaines, un par un.
	Remarque Si l'annuaire Active Directory requiert STARTTLS et que vous ne fournissez pas le certificat, vous ne pouvez pas créer l'annuaire.

- 7 Dans la section Détails de l'utilisateur Bind, entrez les informations d'identification appropriées pour faciliter la synchronisation des annuaires.

Pour Active Directory via LDAP :

Option	Description
Nom unique de base	Entrez le nom unique de base de recherche. Par exemple, cn=users,dc=corp,dc=local .
Nom unique de liaison	Entrez le nom unique de la liaison. Par exemple, cn=fritz infra,cn=users,dc=corp,dc=local

Pour Active Directory (authentification Windows intégrée) :

Option	Description
UPN de l'utilisateur Bind	Entrez le nom principal d'utilisateur de l'utilisateur qui peut s'authentifier auprès du domaine. Par exemple, UserName@example.com .
Mot de passe du nom unique de liaison	Entrez le mot de passe de l'utilisateur Bind.

- 8 Cliquez sur **Tester la connexion** pour tester la connexion vers l'annuaire configuré.

Ce bouton n'est pas présent si vous avez sélectionné Active Directory (authentification Windows intégrée).

- 9 Cliquez sur **Enregistrer et Suivant**.

La page Sélectionnez les domaines apparaît avec la liste des domaines.

- 10 Examinez et mettez à jour les domaines répertoriés pour la connexion Active Directory.

- Pour Active Directory (authentification Windows intégrée), sélectionnez les domaines qui doivent être associés à cette connexion Active Directory.
- Pour Active Directory sur LDAP, les domaines disponibles sont signalés par une coche.


Remarque Si vous ajoutez un domaine d'approbation après la création de l'annuaire, le service ne le détecte pas automatiquement. Pour activer le service afin de détecter le domaine, le connector doit quitter, puis rejoindre le domaine. Lorsque le connector rejoint le domaine, le domaine d'approbation s'affiche dans la liste.

- 11 Cliquez sur **Suivant**.

- 12 Vérifiez que les noms d'attributs de l'annuaire Directories Management sont mappés aux attributs Active Directory appropriés.

Si les noms d'attributs de l'annuaire ne sont pas correctement mappés, sélectionnez le bon attribut Active Directory dans le menu déroulant.

- 13 Cliquez sur **Suivant**.

- 14 Cliquez sur  pour sélectionner les groupes que vous souhaitez synchroniser entre Active Directory et l'annuaire.

Lorsque vous ajoutez un groupe à partir d'Active Directory, si les membres de ce groupe ne figurent pas sur la liste Utilisateurs, ils y sont ajoutés. Lorsque vous synchronisez un groupe, les utilisateurs ne disposant pas du groupe principal Utilisateurs de domaine dans Active Directory ne sont pas synchronisés.

Remarque Le système d'authentification utilisateur Directories Management importe les données provenant d'Active Directory lors de l'ajout des groupes et utilisateurs, et la vitesse du système est limitée par les capacités d'Active Directory. Par conséquent, les opérations d'importation peuvent être assez longues, suivant le nombre de groupes et d'utilisateurs à ajouter. Pour minimiser les retards ou problèmes potentiels, limitez le nombre de groupes et d'utilisateurs à ceux requis pour l'opération vRealize Automation.


Si les performances de votre système déclinent ou si des erreurs se produisent, fermez toutes les applications inutiles et assurez-vous que votre système dispose d'une mémoire suffisante attribuée à Active Directory. Si les problèmes persistent, augmentez cette allocation de mémoire selon les besoins. Pour les systèmes comportant un nombre important d'utilisateurs et de groupes, vous pouvez allouer à Active Directory jusqu'à 24 Go de mémoire.

- 15 Cliquez sur **Suivant**.

- 16 Cliquez sur  pour ajouter des utilisateurs supplémentaires.

Les valeurs appropriées sont comme suit :

- Un seul utilisateur : `CN=username,CN=Users,OU=Users,DC=myCorp,DC=com`
- Plusieurs utilisateurs : `OU=Users,OU=myUnit,DC=myCorp,DC=com`

Pour exclure des utilisateurs, cliquez sur  afin de créer un filtre permettant d'exclure certains types d'utilisateurs. Vous pouvez sélectionner un attribut d'utilisateur à filtrer, la règle de requête et sa valeur.

- 17 Cliquez sur **Suivant**.

- 18 Examinez la page pour voir combien d'utilisateurs et de groupes sont synchronisés avec l'annuaire.

Si vous souhaitez apporter des modifications aux utilisateurs et aux groupes, cliquez sur les liens Modifier.

Remarque Assurez-vous que vous indiquez des noms uniques d'utilisateur qui se trouvent sous le nom unique de base spécifié précédemment. Si un nom unique d'utilisateur se trouve en dehors du nom unique de base, les utilisateurs de ce nom unique seront synchronisés, mais ne pourront pas se connecter.

- 19 Cliquez sur **Transférer vers Workspace** pour lancer la synchronisation avec l'annuaire.

La connexion à Active Directory a réussi et les utilisateurs et groupes sélectionnés sont ajoutés à l'annuaire. Vous pouvez désormais affecter des utilisateurs et des groupes aux rôles appropriés de vRealize Automation en sélectionnant **Administration > Utilisateurs et groupes > Utilisateurs et groupes d'annuaires**. Consultez [Attribuer des rôles à des utilisateurs ou des groupes du répertoire](#) pour plus d'informations.

Suivant

Si votre environnement vRealize Automation est configuré pour la haute disponibilité, vous devez spécifiquement configurer la gestion des annuaires en vue de la haute disponibilité. Reportez-vous à [Configurer Directories Management pour High Availability](#).

- Configurez les méthodes d'authentification. Une fois les utilisateurs et les groupes synchronisés avec l'annuaire, si le connecteur est également utilisé pour l'authentification, vous pouvez configurer des méthodes d'authentification supplémentaires sur le connecteur. Si un tiers est le fournisseur d'identité d'authentification, configurez ce dernier dans le connecteur.
- Examinez la stratégie d'accès par défaut. La stratégie d'accès par défaut est configurée de manière à permettre à tous les dispositifs de l'ensemble des pages réseau d'accéder au navigateur Web, avec un délai d'expiration de session défini sur 8 heures ou pour accéder à une application cliente ayant un délai d'expiration de session de 2 160 heures (90 jours). Vous pouvez modifier la stratégie d'accès par défaut et lorsque vous ajoutez des applications Web au catalogue, vous pouvez créer d'autres stratégies.
- Appliquez des informations de marque personnalisées à la console d'administration, aux pages du portail utilisateur et à l'écran de connexion.

Configurer une connexion à un annuaire OpenLDAP

Vous pouvez configurer une connexion à un annuaire OpenLDAP au moyen de la fonction Gestion des annuaires.

Il existe différents protocoles LDAP, mais OpenLDAP est le seul dont l'utilisation a été testée et approuvée pour la fonctionnalité de gestion d'annuaires de vRealize Automation.

Pour intégrer votre annuaire LDAP, vous créez un annuaire Directories Management correspondant et synchronisez les utilisateurs et les groupes depuis votre annuaire LDAP vers l'annuaire Directories Management. Vous pouvez configurer un planning de synchronisation régulier pour les mises à jour suivantes.

De plus, vous sélectionnez les attributs LDAP que vous voulez synchroniser pour les utilisateurs et les mappez aux attributs Directories Management.

La configuration de votre annuaire LDAP peut être basée sur des schémas par défaut ou vous pouvez avoir créé des schémas personnalisés. Vous pouvez également avoir défini des attributs personnalisés. Pour que Directories Management puisse interroger votre annuaire LDAP afin d'obtenir des objets d'utilisateur ou de groupe, vous devez fournir les filtres de recherche et les noms d'attribut LDAP qui s'appliquent à votre annuaire LDAP.

En particulier, vous devez fournir les informations suivantes.

- Filtres de recherche LDAP pour obtenir des groupes, des utilisateurs et l'utilisateur Bind
- Noms d'attribut LDAP pour l'appartenance au groupe, l'UUID et le nom unique

Prérequis

- Examinez la configuration sur la page Attributs utilisateur et ajoutez tout attribut supplémentaire que vous souhaitez synchroniser. Vous mappez les attributs de Directories Management aux attributs de votre annuaire LDAP lorsque vous créez l'annuaire. Ces attributs sont synchronisés pour les utilisateurs dans l'annuaire.

Remarque Lorsque vous modifiez les attributs utilisateur, tenez compte des effets sur les autres annuaires dans le service. Si vous prévoyez d'ajouter des annuaires Active Directory et LDAP, veillez à ne pas marquer des attributs comme requis à l'exception de **userName**. Les paramètres indiqués sur la page Attributs utilisateur s'appliquent à tous les annuaires dans le service. Si un attribut est marqué comme requis, les utilisateurs ne disposant pas de cet attribut ne sont pas synchronisés avec le service Directories Management.

- Un compte d'utilisateur de nom unique de liaison. Il est recommandé d'utiliser un compte d'utilisateur de nom unique de liaison avec un mot de passe sans date d'expiration.
- Dans votre annuaire LDAP, l'UUID des utilisateurs et des groupes doit être au format de texte brut.
- Dans votre annuaire LDAP, un attribut de domaine doit exister pour tous les utilisateurs et les groupes.

Vous mappez cet attribut à l'attribut Directories Management **domain** lorsque vous créez l'annuaire Directories Management.

- Les noms d'utilisateur ne doivent pas contenir d'espaces. Si un nom d'utilisateur contient une espace, l'utilisateur est synchronisé, mais les droits ne sont pas disponibles pour l'utilisateur.
- Si vous utilisez l'authentification par certificat, les utilisateurs doivent posséder des valeurs pour les attributs `userPrincipalName` et d'adresse électronique.

Procédure

- 1 Sélectionnez **Administration > Gestion des répertoires > Répertoires**.
- 2 Cliquez sur **Ajouter un annuaire** et sélectionnez **Ajouter un annuaire LDAP**.
- 3 Entrez les informations requises sur la page Ajouter un annuaire LDAP.

Option	Description
Nom de l'annuaire	Entrez un nom pour l'annuaire Directories Management.
Synchronisation et authentification de l'annuaire	<p>a Dans le champ Synchroniser le connecteur, sélectionnez le connecteur que vous voulez utiliser pour synchroniser des utilisateurs et des groupes de l'annuaire LDAP avec le répertoire Directories Management.</p> <p>Un composant de connecteur est toujours disponible avec le service Directories Management par défaut. Ce connecteur s'affiche dans la liste déroulante. Si vous installez plusieurs dispositifs Directories Management pour la haute disponibilité, le composant de connecteur de chaque dispositif s'affiche dans la liste.</p> <p>Vous n'avez pas besoin d'un connecteur séparé pour un annuaire LDAP. Un connecteur peut prendre en charge plusieurs annuaires, qu'il s'agisse d'annuaires Active Directory ou LDAP.</p> <p>b Dans le champ Authentification, si vous voulez utiliser cet annuaire LDAP pour authentifier des utilisateurs, sélectionnez Oui.</p> <p>Si vous voulez utiliser un fournisseur d'identité tiers pour authentifier des utilisateurs, sélectionnez Non. Après avoir ajouté la connexion d'annuaire pour synchroniser les utilisateurs et les groupes, accédez à la page Administration > Gestion des annuaires > Fournisseurs d'identité pour ajouter le fournisseur d'identité tiers à des fins d'authentification.</p> <p>c Pour la plupart des configurations, laissez la valeur par défaut Personnalisé sélectionnée dans la zone de texte Attribut de recherche d'annuaire. Dans le champ Attribut de recherche d'annuaire personnalisé, spécifiez l'attribut d'annuaire LDAP à reprendre pour l'utilisateur et les groupes de noms. Cet attribut identifie de façon unique des entités, telles que des utilisateurs et des groupes, provenant du serveur LDAP. Par exemple, cn.</p>
Emplacement du serveur	<p>Entrez le numéro de port et l'hôte du serveur d'annuaire LDAP. Pour l'hôte de serveur, vous pouvez spécifier le nom de domaine complet ou l'adresse IP. Par exemple : monserveurLDAP.exemple.com ou 100.00.00.0.</p> <p>Si vous disposez d'un cluster de serveurs derrière un équilibrage de charge, entrez les informations de ce dernier à la place.</p>

Option	Description
Configuration LDAP	<p>Spécifiez les filtres et les attributs de recherche LDAP que Directories Management peut utiliser pour interroger votre annuaire LDAP. Les valeurs par défaut sont fournies en fonction du schéma LDAP principal.</p> <p>Filtrer les demandes</p> <ul style="list-style-type: none"> ■ Groupes : filtre de recherche pour obtenir des objets de groupe. Par exemple : (objectClass=group) ■ Utilisateur Bind : filtre de recherche pour obtenir l'objet d'utilisateur Bind, c'est-à-dire l'utilisateur pouvant établir la liaison à l'annuaire. Par exemple : (objectClass=person) ■ Utilisateurs : filtre de recherche pour obtenir des utilisateurs à synchroniser. Par exemple : (&(objectClass=user)(objectCategory=person)) <p>Attributs</p> <ul style="list-style-type: none"> ■ Appartenance : attribut utilisé dans votre annuaire LDAP pour définir les membres d'un groupe. Par exemple : membre ■ UUID d'objet : attribut utilisé dans votre annuaire LDAP pour définir l'UUID d'un utilisateur ou d'un groupe. Par exemple : entryUUID ■ Nom unique : attribut utilisé dans votre annuaire LDAP pour le nom unique d'un utilisateur ou d'un groupe. Par exemple : entryDN
Certificats	<p>Si votre annuaire LDAP nécessite un accès SSL, cochez la case Cet annuaire exige que toutes les connexions utilisent SSL. Copiez/collez ensuite le certificat CA SSL racine du serveur d'annuaire LDAP dans la zone de texte Certificat SSL. Vérifiez que le certificat est au format PEM et incluez les lignes « BEGIN CERTIFICATE » et « END CERTIFICATE ».</p> <p>Enfin, assurez-vous que le numéro de port correct est spécifié dans le champ Port serveur dans la section Emplacement du serveur de la page.</p>
Détails de l'utilisateur Bind	<p>Nom unique de base : entrez le nom unique à partir duquel vous souhaitez lancer les recherches. Par exemple, cn=users,dc=example,dc=com</p> <p>Tous les utilisateurs concernés doivent résider sous le nom unique de base. Si ce n'est pas le cas, les utilisateurs non couverts ne pourront pas se connecter, même s'ils appartiennent à l'un des groupes mentionnés.</p> <p>Nom unique de liaison : entrez le nom unique à utiliser pour établir la liaison à l'annuaire LDAP. Vous pouvez entrer des noms d'utilisateur, mais un nom unique convient mieux dans la plupart des déploiements.</p> <p>Remarque Il est recommandé d'utiliser un compte d'utilisateur de nom unique de liaison avec un mot de passe sans date d'expiration.</p> <p>Mot de passe du nom unique de liaison : entrez le mot de passe de l'utilisateur de nom unique de liaison.</p>

- 4 Pour tester la connexion au serveur d'annuaire LDAP, cliquez sur **Tester la connexion**.

Si la connexion échoue, vérifiez les informations que vous avez entrées et effectuez les modifications nécessaires.

- 5 Cliquez sur **Enregistrer et Suivant**.

- 6 Assurez-vous que le domaine correct est sélectionné dans la page de sélection des domaines, puis cliquez sur **Suivant**.
- 7 Sur la page Mapper des attributs, vérifiez que les attributs de Directories Management sont mappés aux bons attributs LDAP.

Ces attributs sont synchronisés pour les utilisateurs.

Important Vous devez spécifier un mappage pour l'attribut **domain**.

Vous pouvez ajouter des attributs à la liste sur la page Attributs utilisateur.

- 8 Cliquez sur **Suivant**.
- 9 Cliquez sur **+** pour sélectionner les groupes à synchroniser depuis l'annuaire LDAP et avec l'annuaire Directories Management dans la page Sélectionner les groupes (utilisateurs) à synchroniser.

Si vous disposez de plusieurs groupes avec le même nom dans votre annuaire LDAP, vous devez spécifier des noms uniques sur la page des groupes.

Lorsque vous ajoutez un groupe à partir d'Active Directory, si les membres de ce groupe ne figurent pas sur la liste Utilisateurs, ils y sont ajoutés. Lorsque vous synchronisez un groupe, les utilisateurs ne disposant pas du groupe principal Utilisateurs de domaine dans Active Directory ne sont pas synchronisés.

L'option **Synchroniser les membres du groupe imbriqué** est activée par défaut. Lorsque cette option est activée, tous les utilisateurs qui appartiennent directement au groupe que vous sélectionnez, ainsi que les utilisateurs qui appartiennent à des groupes imbriqués sous ce groupe, sont synchronisés. Notez que les groupes imbriqués ne sont pas synchronisés ; seuls les utilisateurs qui appartiennent aux groupes imbriqués le sont. Dans l'annuaire Directories Management, ces utilisateurs sont affichés en tant que membres du groupe de niveau supérieur que vous avez sélectionné pour la synchronisation. En effet, la hiérarchie sous un groupe sélectionné est aplatie et les utilisateurs de tous les niveaux apparaissent dans Directories Management en tant que membres du groupe sélectionné.

Si cette option est désactivée, lorsque vous spécifiez un groupe à synchroniser, tous les utilisateurs qui appartiennent directement à ce groupe sont synchronisés. Les utilisateurs qui appartiennent à des groupes imbriqués sous ce groupe ne sont pas synchronisés. La désactivation de cette option est utile pour les configurations d'annuaire importantes pour lesquelles parcourir une arborescence de groupes demande beaucoup de ressources et de temps. Si vous désactivez cette option, veillez à sélectionner tous les groupes dont vous voulez synchroniser les utilisateurs.

Remarque Le système d'authentification utilisateur Directories Management importe les données provenant d'Active Directory lors de l'ajout des groupes et utilisateurs, et la vitesse du système est limitée par les capacités d'Active Directory. Par conséquent, les opérations d'importation peuvent être assez longues, suivant le nombre de groupes et d'utilisateurs à ajouter. Pour minimiser les retards ou problèmes potentiels, limitez le nombre de groupes et d'utilisateurs à ceux requis pour l'opération vRealize Automation.

Si les performances de votre système déclinent ou si des erreurs se produisent, fermez toutes les applications inutiles et assurez-vous que votre système dispose d'une mémoire suffisante attribuée à Gestion des annuaires. Si les problèmes persistent, augmentez cette allocation de mémoire selon les besoins. Pour les systèmes comportant un nombre important d'utilisateurs et de groupes, vous pouvez allouer à Gestion des annuaires jusqu'à 24 Go de mémoire.

10 Cliquez sur **Suivant**.

11 Cliquez sur **+** pour ajouter des utilisateurs supplémentaires. Par exemple, entrez **CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com**.

Vous pouvez inclure des unités d'organisation, telles que les utilisateurs individuels ici.

Vous pouvez créer un filtre permettant d'exclure certains types d'utilisateurs. Sélectionnez un attribut d'utilisateur à filtrer, la règle de requête et sa valeur.

12 Cliquez sur **Suivant**.

13 Examinez la page pour voir combien d'utilisateurs et de groupes se synchroniseront avec l'annuaire et pour voir le planning de synchronisation par défaut.

Pour apporter des modifications aux utilisateurs et aux groupes, ou à la fréquence de synchronisation, cliquez sur les liens **Modifier**.

14 Cliquez sur **Synchroniser l'annuaire** pour démarrer la synchronisation d'annuaire.

La connexion à l'annuaire LDAP est établie et les utilisateurs et les groupes sont synchronisés entre l'annuaire LDAP et l'annuaire Directories Management.

Vous pouvez désormais affecter des utilisateurs et des groupes aux rôles appropriés de vRealize Automation en sélectionnant **Administration > Utilisateurs et groupes > Utilisateurs et groupes d'annuaires**. Consultez [Attribuer des rôles à des utilisateurs ou des groupes du répertoire](#) pour plus d'informations.

Limites de l'intégration d'annuaire LDAP

Il existe plusieurs limitations importantes concernant l'intégration d'annuaire LDAP dans la gestion des répertoires.

- Vous ne pouvez intégrer qu'un environnement d'annuaire LDAP à un seul domaine.
Pour intégrer plusieurs domaines à partir d'un annuaire LDAP, vous devez créer des annuaires Directories Management supplémentaires, un pour chaque domaine.
- Les méthodes d'authentification suivantes ne sont pas prises en charge pour les annuaires Directories Management de type LDAP.
 - authentification Kerberos
 - RSA Adaptive Authentication
 - ADFS en tant que fournisseur d'identité tiers
 - SecurID
 - Authentification Radius avec serveur Vasco et SMS Passcode
- Vous ne pouvez pas joindre un domaine LDAP.
- L'intégration à des ressources View ou publiées Citrix n'est pas prise en charge pour les annuaires Directories Management de type LDAP.
- Les noms d'utilisateur ne doivent pas contenir d'espaces. Si un nom d'utilisateur contient une espace, l'utilisateur est synchronisé, mais les droits ne sont pas disponibles pour l'utilisateur.
- Si vous prévoyez d'ajouter des annuaires Active Directory et LDAP, veillez à ne pas marquer des attributs comme requis sur la page Attributs utilisateur, à l'exception de userName, qui peut être marqué comme requis. Les paramètres sur la page Attributs utilisateur s'appliquent à tous les annuaires dans le service. Si un attribut est marqué comme requis, les utilisateurs sans cet attribut ne sont pas synchronisés avec le service Directories Management.
- Si vous disposez de plusieurs groupes avec le même nom dans votre annuaire LDAP, vous devez spécifier des noms uniques dans le service Directories Management. Vous pouvez spécifier les noms lorsque vous sélectionnez les groupes à synchroniser.
- L'option pour autoriser les utilisateurs à réinitialiser leurs mots de passe expirés n'est pas disponible.
- Le fichier `domain_krb.properties` n'est pas pris en charge.

Configurer Directories Management pour High Availability

Vous pouvez utiliser Directories Management afin de configurer une connexion Active Directory haute disponibilité dans vRealize Automation.

Chaque instance du dispositif vRealize Automation inclut un connecteur qui prend en charge l'authentification de l'utilisateur, bien qu'un seul connecteur soit habituellement configuré pour exécuter la synchronisation d'annuaire. Le choix du connecteur devant faire office de connecteur de synchronisation est sans incidence. Afin de prendre en charge la haute disponibilité pour la fonctionnalité Gestion des

annuaires, configurez un second connecteur qui correspond au second dispositif vRealize Automation. Ce connecteur doit se connecter au fournisseur d'identité et pointer vers la même instance d'Active Directory. Grâce à cette configuration, l'échec d'un dispositif est compensé par la reprise de la gestion de l'authentification de l'utilisateur par l'autre dispositif.

Dans un environnement de haute disponibilité, tous les nœuds doivent servir les mêmes instances d'Active Directory, les mêmes utilisateurs, méthodes d'authentification, etc. Pour ce faire, la méthode la plus directe consiste à promouvoir le fournisseur d'identité auprès du cluster, en définissant l'hôte de l'équilibrage de charge en tant qu'hôte du fournisseur d'identité. Grâce à cette configuration, toutes les demandes d'authentification sont dirigées vers l'équilibrage de charge, qui les transmet à son tour au connecteur approprié.

Prérequis

- Configurez le déploiement de vRealize Automation avec au moins deux instances du dispositif vRealize Automation.
- Installez vRealize Automation en mode Enterprise fonctionnant dans un domaine unique avec deux instances du dispositif vRealize Automation.
- Installez et configurez un équilibrage de charge adapté au déploiement de vRealize Automation.
- Configurez les locataires et la fonctionnalité Gestion des annuaires à l'aide de l'un des connecteurs fournis avec les instances installées du dispositif vRealize Automation. Pour plus d'informations sur la configuration du locataire, reportez-vous à [Configuration des paramètres de locataire](#).

Procédure

- 1 Connectez-vous à l'équilibrage de charge du déploiement vRealize Automation en tant qu'administrateur de locataire.
L'URL de l'équilibrage de charge est `<load balancer address>/vcac/org/tenant_name`.
- 2 Sélectionnez **Administration > Directories Management > Fournisseurs d'identité**.
- 3 Cliquez sur le fournisseur d'identité actuellement utilisé dans le système.
L'annuaire et le connecteur existants qui fournissent une gestion des identités de base s'affichent.
- 4 Sur la page Fournisseur d'identité, cliquez sur la liste déroulante **Ajouter un connecteur**, puis sélectionnez le connecteur correspondant à la seconde instance du dispositif vRealize Automation.
- 5 Dans la zone de texte **Mot de passe du DN de liaison** qui s'affiche à la sélection du connecteur, entrez le mot de passe correspondant.
- 6 Cliquez sur **Ajouter un connecteur**.
- 7 Le connecteur principal s'affiche dans la zone de texte **Nom d'hôte du fournisseur d'identité** par défaut. Changez le nom d'hôte afin qu'il pointe vers l'équilibrage de charge.

Configurer une relation de confiance bidirectionnelle entre vRealize Automation et Active Directory

Vous pouvez améliorer la sécurité du système d'une connexion Active Directory vRealize Automation de base en configurant une relation de confiance bidirectionnelle entre votre fournisseur d'identité et Active Directory Federated Services.

Pour configurer une relation de confiance bidirectionnelle entre vRealize Automation et Active Directory, vous devez créer un fournisseur d'identité personnalisé et ajouter des métadonnées Active Directory à ce fournisseur. Vous devez également modifier la stratégie par défaut utilisée par votre déploiement de vRealize Automation. Enfin, vous devez configurer Active Directory pour reconnaître votre fournisseur d'identité.

Prérequis

- Vérifiez que vous avez configuré des locataires pour votre déploiement de vRealize Automation et défini un lien Active Directory approprié pour prendre en charge l'authentification de base de l'ID et du mot de passe utilisateur Active Directory.
- Active Directory est installé et configuré pour être utilisé sur votre réseau.
- Obtenez les métadonnées Active Directory Federated Services (ADFS) appropriées.
- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

- 1 Obtenez le fichier de métadonnées de fédération.

Vous pouvez télécharger ce fichier sur

<https://servername.domain/FederationMetadata/2007-06/FederationMetadata.xml>

- 2 Recherchez le mot « logout » et modifiez l'emplacement de chaque instance pour pointer vers <https://servername.domain/adfs/ls/logout.aspx>

Par exemple, l'élément suivant :

```
SingleLogoutService
  Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Location="https://servername.domain/adfs/ls/ "/>
```

Doit être remplacé par :

```
SingleLogoutService
  Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Location="https://servername.domain/adfs/ls/logout.aspx"/>
```

3 Créez un nouveau fournisseur d'identité pour votre déploiement.

- a Sélectionnez **Administration > Directories Management > Fournisseurs d'identité**.
- b Cliquez sur **Ajouter un fournisseur d'identité** et remplissez les champs nécessaires.

Option	Description
Nom du fournisseur d'identité	Entrez un nom pour le nouveau fournisseur d'identité
Métadonnées du fournisseur d'identité (URI ou XML)	Collez ici le contenu de votre fichier de métadonnées d'Active Directory Federated Services.
Nommer la stratégie d'ID dans la demande SAML (facultatif)	Le cas échéant, entrez un nom pour la demande SAML de stratégie d'identité.
Utilisateurs	Sélectionnez les domaines pour lesquels vous souhaitez que les utilisateurs disposent de privilèges d'accès.
Traiter les métadonnées IDP	Cliquez pour traiter le fichier de métadonnées que vous avez ajouté.
Réseau	Sélectionnez les plages réseau auxquelles vous souhaitez que les utilisateurs aient accès.
Méthodes d'authentification	Entrez un nom pour la méthode d'authentification utilisée pour ce fournisseur d'identité.
Contexte SAML	Sélectionnez le contexte approprié à votre système.
Certificat de signature SAML	Cliquez sur le lien à côté du titre des métadonnées SAML pour télécharger les métadonnées Gestion des répertoires.

- c Enregistrez le fichier de métadonnées Directories Management sous le nom `sp.xml`.
- d Cliquez sur **Ajouter**.

4 Ajoutez une règle à la stratégie par défaut.

- a Sélectionnez **Administration > Directories Management > Stratégies**.
- b Cliquez sur le nom de la stratégie par défaut.
- c Cliquez sur l'icône + sous l'en-tête **Règles de stratégie** pour ajouter une nouvelle règle.

Utilisez les champs de la page Ajouter une règle de stratégie pour créer une règle qui détermine les méthodes d'authentification primaire et secondaire à utiliser pour une plage réseau et un périphérique spécifiques.

Par exemple, si votre plage réseau est **Ma machine** et si vous devez pouvoir accéder au contenu depuis **Tous les types de périphériques**, alors vous devrez, dans le cas d'un déploiement type, vous authentifier en utilisant la méthode suivante :

Nom d'utilisateur et mot de passe ADFS.

- d Cliquez sur **Enregistrer** pour enregistrer vos stratégies mises à jour.
- e Sur la page Stratégie par défaut, faites glisser la nouvelle règle vers le haut du tableau pour qu'elle soit prioritaire sur les règles existantes.

- 5 À l'aide de la console de gestion Active Directory Federated Services, ou d'un autre outil approprié, définissez une relation de partie de confiance avec le fournisseur d'identité vRealize Automation.

Pour configurer cette relation de confiance, vous devez importer les métadonnées Gestion des annuaires que vous avez précédemment téléchargées. Reportez-vous à la documentation Microsoft Active Directory pour obtenir des informations supplémentaires sur la configuration d'Active Directory Federated Services pour les relations de confiance bidirectionnelles. Dans le cadre de ce processus, vous pouvez également :

- Définir une confiance tierce relais. Lorsque vous configurez cette confiance, vous devez importer le fichier XML de métadonnées du fournisseur de services du fournisseur d'identité VMware que vous avez copié et enregistré.
- Créez une règle de réclamation qui transforme les attributs récupérés depuis LDAP en règle Obtenir des attributs dans le format SAML souhaité. Après avoir créé la règle, modifiez-la en ajoutant le texte suivant :

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer
= c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"vmwareidentity.domain.com");
```

Configurer la fédération SAML entre Directories Management et SSO2

Vous pouvez établir une fédération SAML entre vRealize Automation Directories Management et des systèmes qui utilisent SSO2 pour prendre en charge l'authentification unique.

Établissez la fédération entre Directories Management et SSO2 en créant une connexion SAML entre les deux parties. Actuellement, le seul flux de bout en bout pris en charge est celui où SSO2 agit comme le fournisseur d'identité (IdP) et Directories Management comme le fournisseur de service (SP).

Pour l'authentification utilisateur SSO2, le même compte doit exister dans Directories Management et dans SSO2. Au minimum, l'UPN (UserPrincipalName) de l'utilisateur doit être identique sur les deux extrémités. Les autres attributs peuvent être différents, car ils sont nécessaires pour identifier le sujet SAML.

Pour les utilisateurs locaux de SSO2, comme `admin@vsphere.local`, des comptes correspondants doivent également exister dans Directories Management, où au moins l'UPN de l'utilisateur est identique. Créez ces comptes manuellement ou avec un script utilisant les API de création d'utilisateurs locaux Directories Management.

Configurer SAML entre SSO2 et Directories Management implique de le configurer sur les composants Directories Management et SSO.

Tableau 2-4. Configuration de composant de fédération SAML

Composant	Configuration
Gestion des annuaires	Configurez SSO2 en tant que fournisseur d'identité tiers sur Directories Management et mettez à jour la stratégie d'authentification par défaut. Vous pouvez créer un script automatisé permettant de configurer Directories Management.
Composant SSO2	Configurez Directories Management en tant que fournisseur de service en important le fichier Directories Management sp.xml. Ce fichier vous permet de configurer SSO2 pour utiliser Directories Management en tant que fournisseur de service.

Prérequis

- Configurez des locataires pour votre déploiement vRealize Automation. Reportez-vous à [Créer des locataires supplémentaires](#).
- Configurez un lien Active Directory approprié pour prendre en charge l'authentification de base d'ID utilisateur et de mot de passe Active Directory.
- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

- 1 Téléchargez les métadonnées du fournisseur d'identité SSO2 via l'interface utilisateur SSO2.
 - a Connectez-vous à vCenter en tant qu'administrateur à l'adresse `https://<cloudvm-hostname>/`.
 - b Cliquez sur le lien **Aanmelden bij vSphere Web Client**.
 - c Dans le volet de navigation gauche, sélectionnez **Administration > Single Sign-On > Configuration**.
 - d Cliquez sur l'option **Télécharger** en regard de l'en-tête Métadonnées pour votre fournisseur de service SAML.

Le téléchargement du fichier `vsphere.local.xml` doit commencer.
 - e Copiez le contenu du fichier `vsphere.local.xml`.
- 2 Sur la page Fournisseurs d'identité de gestion des annuaires de vRealize Automation, créez un nouveau fournisseur d'identité.
 - a Connectez-vous à vRealize Automation en tant qu'**administrateur de locataire**.
 - b Sélectionnez **Administration > Directories Management > Fournisseurs d'identité**.

- c Cliquez sur **Ajouter un fournisseur d'identité** et entrez les informations de configuration.

Option	Action
Nom du fournisseur d'identité	Entrez un nom pour le nouveau fournisseur d'identité.
Zone de texte Métadonnées du fournisseur d'identité (URI ou XML)	Collez le contenu de votre fichier de métadonnées idp.xml SSO2 dans la zone de texte et cliquez sur Traiter les métadonnées IDP .
Nommer la stratégie d'ID dans la demande SAML (facultatif)	Entrez <code>http://schemas.xmlsoap.org/claims/UPN</code> .
Utilisateurs	Sélectionnez les domaines pour lesquels vous souhaitez que les utilisateurs disposent de privilèges d'accès.
Réseau	Sélectionnez les plages réseau pour lesquelles vous souhaitez que les utilisateurs disposent de privilèges d'accès. Si vous souhaitez authentifier les utilisateurs depuis une adresse IP, sélectionnez Toutes les plages .
Méthodes d'authentification	Entrez un nom pour la méthode d'authentification. Utilisez ensuite le menu déroulant Contexte SAML à droite pour mapper la méthode d'authentification sur <code>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</code> .
Certificat de signature SAML	Cliquez sur le lien à côté du titre des métadonnées SAML pour télécharger les métadonnées Gestion des répertoires.

- d Enregistrez le fichier de métadonnées Directories Management sous le nom `sp.xml`.
- e Cliquez sur **Ajouter**.
- 3 Mettez à jour la stratégie d'authentification pertinente sur la page Stratégies Directories Management pour rediriger l'authentification vers le fournisseur d'identité SSO2 tiers.
- a Sélectionnez **Administration > Directories Management > Stratégies**.
- b Cliquez sur le nom de la stratégie par défaut.
- c Cliquez sur la méthode d'authentification sous l'en-tête **Règles de stratégie** pour modifier la règle d'authentification existante.
- d Sur la page Modifier une règle de stratégie, remplacez la méthode d'authentification à partir du mot de passe par une méthode appropriée.
Dans ce cas, la méthode doit être SSO2.
- e Cliquez sur **Enregistrer** pour enregistrer vos stratégies mises à jour.
- 4 Dans le volet de navigation gauche, sélectionnez **Administration > Single Sign-On > Configuration** et cliquez sur **Mettre à jour** pour télécharger le fichier `sp.xml` dans vSphere.

Ajouter des utilisateurs ou des groupes à une connexion Active Directory

Vous pouvez ajouter des utilisateurs ou des groupes à une connexion Active Directory existante.

Le système d'authentification des utilisateurs de la gestion des annuaires importe des données de l'annuaire Active Directory lors de l'ajout de groupes et d'utilisateurs. La vitesse du transport des données est limitée par les capacités d'Active Directory. Par conséquent, les actions peuvent être relativement longues selon le nombre de groupes et d'utilisateurs ajoutés. Afin de minimiser les problèmes, limitez les groupes et les utilisateurs aux groupes et utilisateurs requis pour une action vRealize Automation. En cas

de problèmes, fermez les applications inutiles et vérifiez que votre déploiement alloue une capacité de mémoire adéquate à Active Directory. Si les problèmes persistent, augmentez l'allocation de mémoire Active Directory. Pour les déploiements comportant un nombre important d'utilisateurs et de groupes, vous devrez éventuellement allouer jusqu'à 24 Go de mémoire à Active Directory.

Lorsque vous synchronisez un déploiement vRealize Automation avec plusieurs utilisateurs et groupes, vous pouvez observer un délai avant la disponibilité des détails du journal. L'horodatage du fichier journal peut différer de l'heure d'achèvement indiquée sur la console.

Si les membres d'un groupe ne figurent pas dans la liste Utilisateurs, lorsque vous ajoutez le groupe à partir d'Active Directory, les membres sont ajoutés à la liste. Lorsque vous synchronisez un groupe, les utilisateurs ne disposant pas d'Utilisateurs de domaine comme groupe principal dans Active Directory ne sont pas synchronisés.

Remarque Vous ne pouvez pas annuler une action de synchronisation après le démarrage de l'opération.

Prérequis

- Connector installé et code d'activation activé. Sélectionnez les attributs par défaut souhaités et ajoutez des attributs supplémentaires sur la page Attributs utilisateur.
Reportez-vous à la rubrique *Sélection des attributs à synchroniser avec l'annuaire* dans *Configuration de vRealize Automation*.
- Liste des groupes et des utilisateurs Active Directory à synchroniser depuis Active Directory.
- Pour Active Directory via LDAP, les informations requises incluent le nom unique de base, le nom unique de liaison et le mot de passe du nom unique de liaison.
- Pour l'authentification Windows intégrée à Active Directory, les informations requises incluent l'adresse et le mot de passe de l'UPN de l'utilisateur Bind du domaine.
- Si l'accès à Active Directory s'effectue via SSL, une copie du certificat SSL est requise.
- Si vous avez un annuaire Active Directory à forêts multiples intégré à l'authentification Windows et si le groupe local du domaine contient des membres de différentes forêts, procédez comme suit. Ajoutez l'utilisateur Bind au groupe Administrateurs du groupe local du domaine. Si l'utilisateur Bind n'est pas ajouté, ces membres ne seront pas présents dans le groupe local du domaine.
- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

- 1 Sélectionnez **Administration > Gestion des répertoires > Répertoires**.
- 2 Cliquez sur le nom de l'annuaire souhaité.
- 3 Pour accéder aux options de la boîte de dialogue de synchronisation, cliquez sur **Paramètres de synchronisation**.

- 4 Pour changer la configuration des utilisateurs ou des groupes, cliquez sur l'icône correspondante.

Pour modifier la configuration des groupes :

- Pour ajouter des groupes et une ligne pour la définition du nom unique d'un groupe, cliquez sur l'icône +. Entrez le nom unique approprié.
- Pour supprimer une définition d'un nom unique de groupe, cliquez sur l'icône x du nom unique de groupe correspondant.

Pour modifier la configuration des utilisateurs :

- ◆ Pour ajouter des utilisateurs, cliquez sur l'icône + pour ajouter une ligne pour une définition de nom unique d'utilisateur. Entrez le nom unique de l'utilisateur approprié.

Pour supprimer une définition d'un nom unique d'utilisateur, cliquez sur l'icône x du nom unique d'utilisateur souhaité.

- 5 Cliquez sur **Enregistrer** pour enregistrer vos modifications sans synchroniser vos mises à jour immédiatement. Cliquez sur **Enregistrer et synchroniser** pour enregistrer vos modifications et synchroniser vos mises à jour immédiatement.

Sélection des attributs à synchroniser avec l'annuaire

Lorsque vous configurez l'annuaire Directories Management à synchroniser avec Active Directory, vous devez spécifier les attributs utilisateur qui sont synchronisés avec l'annuaire. Avant de configurer l'annuaire, vous pouvez spécifier sur la page Attributs utilisateur, les attributs requis par défaut et, si vous le souhaitez, des attributs supplémentaires à mapper aux attributs Active Directory.

Lorsque vous configurez la page Attributs utilisateur avant la création de l'annuaire, vous pouvez faire passer les attributs par défaut de l'état obligatoire à l'état facultatif, marquer les attributs si nécessaire et ajouter des attributs personnalisés.

Pour obtenir la liste des attributs mappés par défaut, reportez-vous à [Gestion des attributs utilisateur synchronisés à partir d'Active Directory](#).

Une fois l'annuaire créé, vous pouvez faire passer un attribut obligatoire à l'état facultatif, et vous pouvez supprimer des attributs personnalisés. Il n'est pas possible de modifier un attribut pour le faire passer à l'état obligatoire.

Lorsque vous ajoutez d'autres attributs à synchroniser avec l'annuaire, une fois l'annuaire créé, accédez à la page Attributs mappés de l'annuaire pour mapper ces attributs à ceux d'Active Directory.

Procédure

- 1 Connectez-vous à vRealize Automation en tant qu'administrateur système ou administrateur de locataires.
- 2 Cliquez sur l'onglet Administration.
- 3 Sélectionnez **Directories Management > Attributs utilisateur**.
- 4 Dans la section Attributs par défaut, examinez la liste d'attributs obligatoires et apportez les modifications souhaitées pour refléter les attributs obligatoires.

- 5 Dans la section **Attributs**, ajoutez le nom d'attribut de l'annuaire Directories Management à la liste.
- 6 Cliquez sur **Enregistrer**.
L'état d'attribut par défaut est mis à jour et les attributs que vous avez ajoutés sont ajoutés à la liste d'attributs mappés de l'annuaire.
- 7 Une fois l'annuaire créé, accédez à la page Magasins d'identités et sélectionnez l'annuaire.
- 8 Cliquez sur **Paramètres de synchronisation > Attributs mappés**.
- 9 Dans le menu déroulant des attributs que vous avez ajoutés, sélectionnez l'attribut Active Directory à mapper.
- 10 Cliquez sur **Enregistrer**.

L'annuaire est mis à jour lors de sa prochaine synchronisation avec Active Directory.

Ajouter de la mémoire à Directories Management

Vous pouvez ajouter de la mémoire à Directories Management si des connexions Active Directory contiennent une importante quantité d'utilisateurs ou de groupes.

Par défaut, 4 Go de mémoire sont alloués au service de Directories Management, ce qui suffit à de nombreux déploiements de petite à moyenne tailles. Si votre connexion Active Directory comporte une grande quantité d'utilisateurs ou de groupes, vous pouvez accroître l'allocation de mémoire si nécessaire. L'augmentation de la mémoire convient aux systèmes de plus de 100 000 utilisateurs, chacun répartis dans 30 groupes avec 750 groupes en tout. Pour ces systèmes, VMware recommande d'accroître l'allocation de mémoire de Directories Management à 6 Go.

La mémoire de Directories Management est calculée en fonction de la mémoire totale allouée au dispositif vRealize Automation. Le tableau suivant montre les allocations de mémoire des composants pertinents.

Tableau 2-5. Allocation de mémoire du dispositif vRealize Automation

Mémoire du dispositif virtuel	Mémoire du service vRA	Mémoire du service vIDM
18 Go	3,3 Go	4 Go
24 Go	4,9 Go	6 Go
30 Go	7,4 Go	9,1 Go

Remarque Ces allocations supposent que tous les services par défaut sont activés et en cours d'exécution sur le dispositif virtuel. L'arrêt de certains services peut entraîner leur modification.

Prérequis

- Une connexion Active Directory appropriée est configurée et en cours d'exécution dans le déploiement de vRealize Automation.

Procédure

- 1 Arrêtez les machines sur lesquelles le dispositif vRealize Automation est en cours d'exécution.

- 2 Augmentez l'allocation de mémoire du dispositif virtuel sur chaque machine.

Si vous utilisez l'allocation de mémoire par défaut de 18 Go, VMware recommande de l'accroître à 24 Go.

- 3 Redémarrez les machines du dispositif vRealize Automation.

Créer un fichier de recherche d'hôtes de domaine pour remplacer la recherche de l'emplacement du service DNS (SRV)

Lorsque vous activez l'authentification Windows intégrée, la configuration de l'annuaire est modifiée pour activer le champ Emplacement du service DNS. La recherche de l'emplacement de service connector n'est pas sensible au site. Pour remplacer la sélection DC aléatoire, vous pouvez créer un fichier nommé `domain_krb.properties` et ajouter le domaine aux valeurs des hôtes qui ont priorité sur la recherche SRV.

Procédure

- 1 À partir de la ligne de commande `appliance-va`, connectez-vous en tant qu'utilisateur disposant de privilèges racine.
- 2 Remplacez les répertoires par `/usr/local/horizon/conf` et créez un fichier nommé `domain_krb.properties`.
- 3 Modifiez le fichier `domain_krb.properties` pour ajouter la liste du domaine aux valeurs des hôtes. Ajoutez les informations sous la forme `<AD Domain>=<host:port>`, `<host2:port2>`, `<host2:port2>`.

Par exemple, entrez la liste sous la forme `example.com=examplehost.com:636`, `examplehost2.example.com:389`
- 4 Remplacez le propriétaire du fichier `domain_krb.properties` par `horizon` et le groupe par `www`. Entrez `chown horizon:www /usr/local/horizon/conf/domain_krb.properties`.
- 5 Redémarrez le service. Entrez `service horizon-workspace restart`.

Gestion des attributs utilisateur synchronisés à partir d'Active Directory

La page Attributs utilisateur de la fonctionnalité Directories Management répertorie les attributs utilisateur qui se synchronisent à votre connexion Active Directory.

Les modifications effectuées et sauvegardées sur la page Attributs utilisateur sont ajoutées sur la page Attributs mappés dans le répertoire de Directories Management. Les modifications des attributs sont mises à jour dans le répertoire lors de la synchronisation suivante à Active Directory.

La page Attributs utilisateur répertorie les attributs d'annuaire par défaut pouvant être mappés aux attributs Active Directory. Vous devez sélectionner les attributs requis et ajouter les autres attributs Active Directory que vous souhaitez synchroniser avec l'annuaire.

Tableau 2-6. Attributs Active Directory par défaut à synchroniser avec le répertoire

Nom de l'attribut de l'annuaire	Mappage par défaut vers l'attribut Active Directory
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeId	employeeID
Contrôleur	canonicalName. Ajoute le nom de domaine complet de l'objet.
disabled (utilisateur externe désactivé)	userAccountControl. Indiqué par UF_Account_Disable Lorsqu'un compte est désactivé, les utilisateurs ne peuvent pas se connecter pour accéder à leurs applications et à leurs ressources. Comme les ressources attribuées aux utilisateurs ne sont pas supprimées du compte, lorsque l'indicateur est supprimé du compte, les utilisateurs peuvent se connecter et accéder aux ressources qui leur sont octroyées.
phone	telephoneNumber
lastName	sn
firstName	givenName
email	mail
userName	sAMAccountName

La page Attributs utilisateur répertorie les attributs d'annuaire par défaut pouvant être mappés aux attributs Active Directory. Vous devez sélectionner les attributs requis et ajouter les autres attributs Active Directory que vous souhaitez synchroniser avec l'annuaire.

Tableau 2-7. Attributs Active Directory par défaut à synchroniser avec le répertoire

Nom de l'attribut de l'annuaire	Mappage par défaut vers l'attribut Active Directory
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeId	employeeID
Contrôleur	canonicalName. Ajoute le nom de domaine complet de l'objet.
disabled (utilisateur externe désactivé)	userAccountControl. Indiqué par UF_Account_Disable Lorsqu'un compte est désactivé, les utilisateurs ne peuvent pas se connecter pour accéder à leurs applications et à leurs ressources. Comme les ressources attribuées aux utilisateurs ne sont pas supprimées du compte, lorsque l'indicateur est supprimé du compte, les utilisateurs peuvent se connecter et accéder aux ressources qui leur sont octroyées.
phone	telephoneNumber
lastName	sn
firstName	givenName
email	mail
userName	sAMAccountName

Gestion des connecteurs et des clusters de connecteurs

La page Connecteurs répertorie les connecteurs déployés pour le réseau d'entreprise. Un connecteur synchronise les données des utilisateurs et des groupes entre Active Directory et le service Directories Management. Lorsque ce connecteur est utilisé comme fournisseur d'identité, il authentifie les utilisateurs auprès du service.

Dans vRealize Automation, chaque dispositif vRealize Automation contient son propre connecteur et les connecteurs sont adaptés à la plupart des déploiements.

Lorsque vous associez un annuaire à une instance de connecteur, le connecteur crée une partition pour l'annuaire associé, appelée travailleur. Une instance de connecteur peut avoir plusieurs travailleurs associés. Chaque travailleur fait office de fournisseur d'identité. Le connecteur synchronise les données des utilisateurs et des groupes entre Active Directory et le service au moyen d'un ou de plusieurs travailleurs. Définissez et configurez les méthodes d'authentification par travailleur.

La page Connecteurs vous permet de gérer plusieurs aspects d'un lien Active Directory. Elle contient un tableau et plusieurs boutons offrant la possibilité de réaliser diverses tâches de gestion.

- Dans la colonne Travailleur, sélectionnez un travailleur pour consulter les détails du connecteur et accédez à la page Adaptateurs d'authentification pour afficher l'état des méthodes d'authentification disponibles. Pour plus d'informations sur l'authentification, reportez-vous à la section [Intégration d'autres produits d'authentification de l'utilisateur à Directories Management](#).
- Dans la colonne Fournisseur d'identité, sélectionnez l'IdP à afficher, à modifier ou à désactiver. Reportez-vous à [Configurer une connexion de fournisseur d'identité tiers](#).
- Dans la colonne Annuaire associé, accédez à l'annuaire associé à ce travailleur.
- Pour joindre le connecteur à un domaine Active Directory spécifique, cliquez sur **Joindre le domaine**. Par exemple, lorsque vous configurez l'authentification Kerberos, vous devez joindre le domaine Active Directory contenant des utilisateurs ou ayant une relation d'approbation avec les domaines contenant des utilisateurs.
- Lorsque vous configurez un annuaire avec un environnement Active Directory à authentification Windows intégrée, le connecteur joint le domaine en fonction des détails de configuration.

Connecteurs dans un environnement en cluster

Dans un déploiement vRealize Automation distribué, tous les connecteurs disponibles effectuent toute autorisation utilisateur requise, alors qu'un seul connecteur désigné gère toute la synchronisation de la configuration. En général, la synchronisation inclut les ajouts, les suppressions ou les modifications apportés à la configuration de l'utilisateur, et elle s'effectue automatiquement à condition que tous les connecteurs soient disponibles. Dans certaines situations, la synchronisation automatique risque de ne pas se produire.

Pour les modifications relatives à la configuration d'annuaires, tels que le nom unique de base, vRealize Automation tente d'envoyer automatiquement les mises à jour à tous les connecteurs d'un cluster. Si un connecteur est inutilisable ou inaccessible pour une raison quelconque, ce connecteur ne recevra pas la mise à jour, même lorsqu'il revient en ligne. Pour mettre en œuvre des modifications de configuration sur des connecteurs qui ne les ont peut-être pas reçues automatiquement, les administrateurs système doivent manuellement enregistrer les modifications sur tous les connecteurs applicables.

Pour les modifications associées au profil de synchronisation d'annuaire, vRealize Automation tente aussi d'envoyer automatiquement les mises à jour à tous les connecteurs. Si le connecteur de synchronisation est opérationnel, la mise à jour est enregistrée et envoyée à tous les connecteurs d'autorisation disponibles. Si un ou plusieurs connecteurs ne sont pas accessibles, l'administrateur système reçoit un avertissement indiquant que certains connecteurs n'ont pas été mis à jour. Si le connecteur de synchronisation n'est pas opérationnel, la mise à jour échoue et une erreur se produit. Si l'administrateur système modifie le connecteur désigné comme connecteur de synchronisation, le nouveau connecteur de synchronisation reçoit les toutes dernières informations de profil disponibles, et ces informations sont envoyées à tous les connecteurs applicables et disponibles.

Joindre une machine de connecteur à un domaine

Dans certains cas, vous devrez éventuellement joindre à un domaine une machine contenant un connecteur de la gestion des annuaires.

Pour les annuaires Active Directory via LDAP, vous pouvez joindre un domaine après la création de l'annuaire. Pour les annuaires de type Active Directory (authentification Windows intégrée), le connecteur est joint au domaine automatiquement lorsque vous créez l'annuaire. Dans les deux cas, vous devez fournir les informations d'identification appropriées.

Pour joindre un domaine, vous avez besoin d'informations d'identification Active Directory avec le privilège pour « joindre un ordinateur au domaine AD ». Cela est configuré dans Active Directory avec les droits suivants :

- Créer des objets Ordinateur
- Supprimer des objets Ordinateur

Lorsque vous joignez un domaine, un objet Ordinateur est créé dans l'emplacement par défaut dans Active Directory.

Si vous n'avez pas les droits requis pour joindre un domaine ou si la stratégie de votre entreprise nécessite un emplacement personnalisé pour l'objet Ordinateur, vous devez demander à votre administrateur de créer l'objet et de joindre ensuite la machine du connecteur au domaine.

Procédure

- 1 Demandez à votre administrateur Active Directory de créer l'objet Ordinateur dans Active Directory dans un emplacement déterminé par votre stratégie d'entreprise. Vous devez fournir le nom d'hôte du connecteur. Vérifiez que vous fournissez le nom de domaine complet, par exemple, `server.example.com`.

Vous pouvez trouver le nom d'hôte dans la colonne Nom d'hôte sur la page Connecteurs dans la console d'administration. Sélectionnez **Administration > Directories Management > Connecteurs**.

- 2 Après la création de l'objet Ordinateur, cliquez sur **Joindre un domaine** sur la page Connecteurs pour joindre un domaine en utilisant un compte utilisateur de domaine disponible dans la gestion des annuaires.

À propos de la sélection des contrôleurs de domaine

Le fichier `domain_krb.properties` détermine les contrôleurs de domaine qui sont utilisés pour les annuaires sur lesquels la recherche de l'emplacement du service DNS (enregistrements SRV) est activée. Il contient une liste de contrôleurs de domaine pour chaque domaine. Le connecteur crée le fichier, et vous devez le gérer par la suite. Le fichier remplace la recherche de l'emplacement du service DNS (SRV).

La recherche de l'emplacement du service DNS est activée sur les types d'annuaires suivants :

- Active Directory sur LDAP avec l'option **Cet annuaire prend en charge l'emplacement du service DNS** sélectionnée
- Active Directory (authentification Windows intégrée), pour lequel la recherche de l'emplacement du service DNS est toujours activée

La première fois que vous créez un annuaire sur lequel la recherche de l'emplacement du service DNS est activée, un fichier `domain_krb.properties` est automatiquement créé dans le répertoire `/usr/local/horizon/conf` de la machine virtuelle, puis rempli avec des contrôleurs de domaine pour chaque domaine. Pour remplir le fichier, le connecteur tente de rechercher les contrôleurs de domaine qui se trouvent sur le même site que le connecteur et en sélectionne deux qui sont accessibles et qui réagissent le plus vite.

Lorsque vous créez des annuaires supplémentaires sur lesquels la recherche de l'emplacement du service DNS est activée, ou lorsque vous ajoutez de nouveaux domaines à un annuaire Authentification Windows intégrée, les nouveaux domaines, et une liste de leurs contrôleurs de domaine, sont ajoutés au fichier.

Vous pouvez remplacer la sélection par défaut à tout moment en modifiant le fichier `domain_krb.properties`. Après avoir créé un annuaire, il vous est conseillé de consulter le fichier `domain_krb.properties` et de vérifier que les contrôleurs de domaine répertoriés sont les plus adaptés à votre configuration. Pour un déploiement Active Directory global avec plusieurs contrôleurs de domaine dans différents emplacements géographiques, le fait d'utiliser un contrôleur de domaine proche du connecteur garantit une communication plus rapide avec Active Directory.

Vous devez également mettre à jour le fichier manuellement pour toute autre modification. Les règles suivantes s'appliquent.

- Le fichier `domain_krb.properties` est créé dans la machine virtuelle qui contient le connecteur. Dans un déploiement classique, sans connecteurs supplémentaires déployés, le fichier est créé dans la machine virtuelle de service Directories Management. Si vous utilisez un connecteur supplémentaire pour l'annuaire, le fichier est créé dans la machine virtuelle de connecteur. Une machine virtuelle ne peut contenir qu'un seul fichier `domain_krb.properties`.
- Le fichier est créé et rempli automatiquement avec des contrôleurs de domaine pour chaque domaine, la première fois que vous créez un annuaire sur lequel la recherche de l'emplacement du service DNS est activée.
- Les contrôleurs de domaine de chaque domaine sont classés par ordre de priorité. Pour se connecter à Active Directory, le connecteur teste le premier contrôleur de domaine de la liste. S'il n'est pas accessible, il teste le deuxième de la liste, etc.
- Le fichier est mis à jour uniquement lorsque vous créez un annuaire sur lequel la recherche de l'emplacement du service DNS est activée ou lorsque vous ajoutez un domaine à un annuaire Authentification Windows intégrée. Le nouveau domaine et une liste de contrôleurs de domaine le concernant sont ajoutés au fichier.

Notez que si une entrée pour un domaine existe déjà dans le fichier, elle n'est pas mise à jour. Par exemple, si vous avez créé puis supprimé un annuaire, l'entrée de domaine d'origine reste dans le fichier et elle n'est pas mise à jour.

- Le fichier n'est mis à jour automatiquement dans aucun autre scénario. Par exemple, si vous supprimez un annuaire, l'entrée de domaine n'est pas supprimée du fichier.
- Si un contrôleur de domaine répertorié dans le fichier n'est pas accessible, modifiez le fichier et supprimez-le.
- Si vous ajoutez ou supprimez une entrée de domaine manuellement, vos modifications ne seront pas remplacées.

Mode de sélection des contrôleurs de domaine pour remplir automatiquement le fichier `domain_krb.properties`

Pour remplir automatiquement le fichier `domain_krb.properties`, des contrôleurs de domaine sont sélectionnés en déterminant le sous-réseau sur lequel réside le connecteur (en fonction de l'adresse IP et du masque de réseau), puis en utilisant la configuration Active Directory afin d'identifier le site de ce sous-réseau, en obtenant la liste de contrôleurs de domaine de ce site, en filtrant la liste pour le domaine approprié et en choisissant les deux contrôleurs de domaine qui réagissent le plus vite.

Pour détecter les contrôleurs de domaine qui sont les plus proches, VMware Identity Manager a les exigences suivantes :

- Le sous-réseau du connecteur doit être présent dans la configuration Active Directory, ou un sous-réseau doit être spécifié dans le fichier `runtime-config.properties`.

Le sous-réseau est utilisé pour déterminer le site.

- La configuration Active Directory doit être liée au site.

Si le sous-réseau ne peut pas être déterminé ou si votre configuration Active Directory n'est pas liée au site, la recherche de l'emplacement du service DNS est utilisée pour rechercher des contrôleurs de domaine, et le fichier est rempli avec quelques contrôleurs de domaine qui sont accessibles. Notez qu'il est possible que ces contrôleurs de domaine ne se trouvent pas dans le même emplacement géographique que le connecteur, ce qui peut entraîner des retards ou des délais d'expiration lors de la communication avec Active Directory. Dans ce cas, modifiez le fichier `domain_krb.properties` manuellement et spécifiez les contrôleurs de domaine corrects à utiliser pour chaque domaine.

Exemple de fichier `domain_krb.properties`

```
example.com=host1.example.com:389,host2.example.com:389
```

- [Remplacer la sélection de sous-réseau par défaut](#)

Pour remplir automatiquement le fichier `domain_krb.properties`, le connecteur tente de rechercher les contrôleurs de domaine qui se trouvent sur le même site afin qu'il y ait une latence minimale entre le connecteur et Active Directory.

- [Modifier le fichier `domain_krb.properties`](#)

Le fichier `/usr/local/horizon/conf/domain_krb.properties` détermine les contrôleurs de domaine à utiliser pour les annuaires sur lesquels la recherche de l'emplacement du service DNS est activée. Vous pouvez modifier le fichier à tout moment pour changer la liste de contrôleurs de domaine d'un domaine ou pour ajouter ou supprimer des entrées de domaine. Vos modifications ne seront pas remplacées.

- [Dépannage du fichier `domain_krb.properties`](#)

Utilisez ces informations pour dépanner le fichier `domain_krb.properties`.

Remplacer la sélection de sous-réseau par défaut

Pour remplir automatiquement le fichier `domain_krb.properties`, le connecteur tente de rechercher les contrôleurs de domaine qui se trouvent sur le même site afin qu'il y ait une latence minimale entre le connecteur et Active Directory.

Pour rechercher le site, le connecteur détermine le sous-réseau sur lequel il réside, en fonction de son adresse IP et de son masque de réseau, puis utilise la configuration Active Directory pour identifier le site pour ce sous-réseau. Si le sous-réseau de la machine virtuelle ne se trouve pas dans Active Directory, ou si vous voulez remplacer la sélection de sous-réseau automatique, vous pouvez spécifier un sous-réseau dans le fichier `runtime-config.properties`.

Procédure

- 1 Connectez-vous à la machine virtuelle de Directories Management en tant qu'utilisateur racine.

Remarque Si vous utilisez un connecteur supplémentaire pour l'annuaire, connectez-vous à la machine virtuelle de connecteur.

- 2 Modifiez le fichier `/usr/local/horizon/conf/runtime-config.properties` pour ajouter l'attribut suivant.

`siteaware.subnet.override=subnet`

où *subnet* est un sous-réseau du site dont vous voulez utiliser les contrôleurs de domaine. Par exemple :

`siteaware.subnet.override=10.100.0.0/20`

- 3 Enregistrez et fermez le fichier.
- 4 Redémarrez le service.

```
service horizon-workspace restart
```

Modifier le fichier `domain_krb.properties`

Le fichier `/usr/local/horizon/conf/domain_krb.properties` détermine les contrôleurs de domaine à utiliser pour les annuaires sur lesquels la recherche de l'emplacement du service DNS est activée. Vous pouvez modifier le fichier à tout moment pour changer la liste de contrôleurs de domaine d'un domaine ou pour ajouter ou supprimer des entrées de domaine. Vos modifications ne seront pas remplacées.

Le fichier est créé et rempli automatiquement par le connecteur. Vous devez le mettre à jour manuellement dans certains scénarios.

- Si les contrôleurs de domaine sélectionnés par défaut ne sont pas les plus adaptés à votre configuration, modifiez le fichier et spécifiez les contrôleurs de domaine à utiliser.
- Si vous supprimez un répertoire, supprimez l'entrée de domaine correspondante dans le fichier.
- Si des contrôleurs de domaine dans le fichier ne sont pas accessibles, supprimez-les du fichier.

Reportez-vous également à la section [À propos de la sélection des contrôleurs de domaine](#).

Procédure

- 1 Connectez-vous à la machine virtuelle de Directories Management en tant qu'utilisateur racine.

Remarque Si vous utilisez un connecteur supplémentaire pour l'annuaire, connectez-vous à la machine virtuelle de connecteur.

- 2 Modifiez les annuaires sur `/usr/local/horizon/conf`.
- 3 Modifiez le fichier `domain_krb.properties` pour ajouter ou modifier la liste de domaine aux valeurs d'hôte.

Utilisez le format suivant :

domain=host:port,host2:port,host3:port

Par exemple :

example.com=examplehost1.example.com:389,examplehost2.example.com:389

Répertoriez les contrôleurs de domaine par ordre de priorité. Pour se connecter à Active Directory, le connecteur teste le premier contrôleur de domaine de la liste. S'il n'est pas accessible, il teste le deuxième de la liste, etc.

Important Les noms de domaine doivent être en minuscules.

- 4 Remplacez le propriétaire du fichier `domain_krb.properties` par `horizon` et le groupe par `www` à l'aide de la commande suivante.

```
chown horizon:www /usr/local/horizon/conf/domain_krb.properties
```

- 5 Redémarrez le service.

```
service horizon-workspace restart
```

Dépannage du fichier `domain_krb.properties`

Utilisez ces informations pour dépanner le fichier `domain_krb.properties`.

Erreur « Erreur lors de la résolution du domaine »

Si le fichier `domain_krb.properties` comporte déjà une entrée pour un domaine et si vous tentez de créer un annuaire d'un type différent pour le même domaine, une erreur « Erreur lors de la résolution du domaine » se produit. Vous devez modifier le fichier `domain_krb.properties` et supprimer manuellement l'entrée de domaine avant de créer l'annuaire.

Des contrôleurs de domaine sont inaccessibles

Une fois l'entrée de domaine ajoutée au fichier `domain_krb.properties`, elle n'est pas mise à jour automatiquement. Si des contrôleurs de domaine répertoriés dans le fichier deviennent inaccessibles, modifiez le fichier manuellement et supprimez-les.

Gestion des stratégies d'accès

Les stratégies Directories Management sont des ensembles de règles qui spécifient les critères à respecter pour que les utilisateurs accèdent à leur portail d'applications ou pour lancer des applications Web spécifiques.

Vous créez une règle dans le cadre d'une stratégie. Chaque règle de stratégie peut indiquer les informations suivantes.

- La plage réseau, à partir de laquelle les utilisateurs sont autorisés à se connecter, par exemple à l'intérieur ou à l'extérieur du réseau de l'entreprise.
- Le type de dispositif pouvant accéder au moyen de cette stratégie.
- L'ordre dans lequel les méthodes d'authentification activées sont appliquées.
- Le nombre d'heures pendant lesquelles l'authentification est valide.

- Le message d'accès refusé personnalisé.

Remarque Les stratégies ne contrôlent pas la durée d'une session d'application Web. Elles contrôlent plutôt la durée de la période pendant laquelle les utilisateurs peuvent lancer une application Web.

Le service Directories Management comprend une stratégie par défaut que vous pouvez modifier. Cette stratégie contrôle globalement l'accès au service. Voir [Application de la stratégie d'accès par défaut](#). Pour contrôler l'accès à des applications Web spécifiques, vous pouvez créer des stratégies supplémentaires. Si vous n'appliquez pas de stratégie à une application Web, la stratégie par défaut s'applique.

Configuration de paramètres de stratégie d'accès

Une stratégie contient une ou plusieurs règles d'accès. Chaque règle est composée de paramètres que vous pouvez configurer afin de gérer l'accès des utilisateurs à leurs portails d'application de façon globale ou à des applications Web spécifiées.

Plage réseau

Pour chaque règle, vous déterminez la base d'utilisateurs en spécifiant une plage réseau. Une plage réseau est composée d'une ou de plusieurs plages d'adresses IP. Vous pouvez créer des plages réseau depuis l'onglet Gestion des identités et des accès, Configuration > Plages réseau avant de configurer les ensembles de stratégies d'accès.

Type de périphérique

Sélectionnez le type de périphérique géré par la règle. Les types de clients sont : navigateur Web, l'application Identity Manager Client, iOS, Android et Tous les types de périphériques.

Méthodes d'authentification

Définissez la priorité des méthodes d'authentification pour la règle de stratégie. Les méthodes d'authentification sont appliquées dans l'ordre où elles sont répertoriées. La première instance du fournisseur d'identité qui répond à la méthode d'authentification et à la configuration de la plage réseau de la stratégie est sélectionnée, et la demande d'authentification de l'utilisateur est transmise à l'instance du fournisseur d'identité pour authentification. Si l'authentification échoue, la méthode d'authentification suivante dans la liste est sélectionnée. Si l'authentification par certificat est utilisée, cette méthode d'authentification doit être la première de la liste.

Vous pouvez configurer des règles de stratégie d'accès pour exiger que les utilisateurs fournissent des informations d'identification via deux méthodes d'authentification avant de pouvoir se connecter. Si une méthode d'authentification, ou les deux, échoue et que des méthodes de secours sont également configurées, les utilisateurs sont invités à entrer leurs informations d'identification pour les méthodes d'authentification configurées suivantes. Les deux scénarios suivants décrivent comment le chaînage d'authentification peut fonctionner.

- Dans le premier scénario, la règle de stratégie d'accès est configurée pour exiger que les utilisateurs s'authentifient avec leur mot de passe et avec leurs informations d'identification Kerberos. L'authentification de secours est configurée pour exiger le mot de passe et les informations d'identification RADIUS pour l'authentification. Un utilisateur entre le mot de passe correctement,

mais ne parvient pas à entrer les bonnes informations d'identification Kerberos. Comme l'utilisateur a entré le mot de passe correct, la demande d'authentification de secours ne concerne que les informations d'identification RADIUS. L'utilisateur n'a pas besoin d'entrer de nouveau le mot de passe.

- Dans le second scénario, la règle de stratégie d'accès est configurée pour exiger que les utilisateurs s'authentifient avec leur mot de passe et avec leurs informations d'identification Kerberos. L'authentification de secours est configurée pour exiger RSA SecurID et RADIUS pour l'authentification. Un utilisateur entre le mot de passe correctement, mais ne parvient pas à entrer les bonnes informations d'identification Kerberos. La demande d'authentification de secours concerne les informations d'identification RSA SecurID et RADIUS pour l'authentification.

Durée de la session d'authentification

Pour chaque règle, vous définissez la durée pendant laquelle l'authentification est valide. La valeur détermine la période maximale dont disposent les utilisateurs depuis leur dernier événement d'authentification pour accéder à leur portail ou pour lancer une application Web spécifique. Par exemple, une valeur de 4 dans une règle d'application Web donne aux utilisateurs quatre heures pour lancer l'application Web sans devoir initier un autre événement d'authentification qui étend la durée.

Message d'erreur d'accès refusé personnalisé

Lorsque des utilisateurs tentent de se connecter, mais échouent à cause d'informations d'identification non valides, d'une configuration incorrecte ou d'une erreur système, un message d'accès refusé s'affiche. Le message par défaut est

Accès refusé, car aucune méthode d'authentification valide n'a été trouvée.

Vous pouvez créer un message d'erreur personnalisé pour chaque règle de stratégie d'accès qui remplace le message par défaut. Le message personnalisé peut comporter du texte et un lien pour un message d'appel à l'action. Par exemple, dans une règle de stratégie pour des périphériques mobiles que vous voulez gérer, si un utilisateur essaie de se connecter à partir d'un périphérique désinscrit, le message d'erreur personnalisé suivant peut s'afficher :

Inscrivez votre périphérique pour accéder à des ressources d'entreprise en cliquant sur le lien à la fin de ce message. Si votre périphérique est déjà inscrit, contactez le support pour obtenir de l'aide.

Exemple de stratégie par défaut

La stratégie suivante est un exemple de configuration de la stratégie par défaut pour contrôler l'accès au portail d'applications. Reportez-vous à [Gérer la stratégie d'accès de l'utilisateur](#).

Les règles de stratégie sont évaluées dans l'ordre indiqué. Vous pouvez modifier l'ordre de la stratégie en effectuant un Glisser-déposer de la règle dans la section Règles de stratégie.

Dans le cas d'utilisation suivant, cet exemple de stratégie s'applique à toutes les applications.

STRATÉGIE PAR DÉFAUT

* Nom de stratégie: default_access_policy_set

Description: Default access policy set

S'applique à: Toutes les applications

Règles de la stratégie

Il est possible de créer une liste de règles permettant d'accéder à ces applications Web. Pour chaque règle, sélectionnez la plage de réseau IP, le type de périphériques pouvant accéder aux applications, les méthodes et l'ordre d'authentification, ainsi que la durée maximale en heures pendant laquelle les utilisateurs peuvent utiliser l'application sans devoir s'authentifier de nouveau.

Plage réseau	Type de périphérique	Méthode d'authentification	Nouvelle authentification	
TOUTES LES PLAGES	Navigateur Web	Password	8 Heure(s)	✗ +
TOUTES LES PLAGES	Application du client Identity Manager	Password	2160 Heure(s)	✗ +

Enregistrer Annuler

- Pour le réseau interne (plage de réseau interne), deux méthodes d'authentification sont configurées pour la règle, l'authentification Kerberos et par mot de passe, comme méthode de secours. Pour accéder au portail d'applications depuis un réseau interne, le service tente d'authentifier les utilisateurs d'abord avec l'authentification Kerberos, car il s'agit de la première méthode d'authentification répertoriée dans la règle. Si cela échoue, les utilisateurs sont invités à entrer leur mot de passe Active Directory. Les utilisateurs se connectent à l'aide d'un navigateur et ont maintenant accès à leurs portails utilisateur pendant une session de huit heures.
 - Pour l'accès depuis le réseau externe (Toutes les plages), une seule méthode d'authentification est configurée, RSA SecurID. Pour accéder au portail d'applications depuis un réseau externe, les utilisateurs doivent se connecter avec SecurID. Les utilisateurs se connectent à l'aide d'un navigateur et ont maintenant accès à leurs portails d'applications pendant une session de quatre heures.
- Lorsqu'un utilisateur tente d'accéder à une ressource (sauf s'il s'agit d'applications Web couvertes par une stratégie spécifique à une application Web), la stratégie d'accès au portail par défaut s'applique. Par exemple, la durée de ré-authentification pour ces ressources correspond à la durée de ré-authentification de la règle de stratégie d'accès par défaut. Si la durée pour un utilisateur qui se connecte au portail d'applications est de huit heures conformément à la règle de stratégie d'accès par défaut, lorsque l'utilisateur tente de lancer une ressource pendant la session, l'application se lance sans demander à l'utilisateur de s'authentifier à nouveau.


Gestion des stratégies spécifiques à une application Web

Lorsque vous ajoutez des applications Web au catalogue, vous pouvez créer des stratégies d'accès spécifique à une application Web. Par exemple, vous pouvez créer une stratégie de règles pour une application Web qui spécifie les adresses IP ayant accès à l'application, les méthodes d'authentification à utiliser et l'intervalle au terme duquel une réauthentification est requise.

La stratégie spécifique à une application Web suivante fournit un exemple de stratégie que vous pouvez créer pour contrôler l'accès aux applications Web spécifiées.


Exemple 1 Stratégie spécifique à une application Web stricte

Dans cet exemple, une nouvelle stratégie est créée et appliquée à une application Web sensible.



Sensitive Web Application

To be applied to Web application that should have limited access.


[Supprimer la stratégie](#)

Nom de stratégie*

Sensitive Web Application

Description

To be applied to Web application that should have limited access.

S'applique à

Sélectionnez les applications de votre catalogue auxquelles cette stratégie s'applique.

AirWatch
Content Locker

[Modifier les applications](#)

Règles de la stratégie

Il est possible de créer une liste de règles permettant d'accéder à ces applications. Pour chaque règle, sélectionnez la plage de réseau IP, le type de périphériques pouvant accéder aux applications, les méthodes et l'ordre d'authentification, ainsi que la durée maximale en heures pendant laquelle les utilisateurs peuvent utiliser l'application sans devoir s'authentifier de nouveau.

Plage réseau	Type de périphér...	Méthode d'authe...	Nouvelle authe...	Groupes	
Internal Network	Navigateur Web	Essayez d'abord : Kerberos et 1 recours de plus...	8 Heure(s)	Tous les utilisateurs	✖ +
TOUTES LES PLAGES	Navigateur Web	Securid	4 Heure(s)	Tous les utilisateurs	✖ +

[Enregistrer](#) [Annuler](#)

- 1 Pour accéder au service depuis l'extérieur du réseau d'entreprise, l'utilisateur doit se connecter à l'aide de RSA SecurID. L'utilisateur se connecte via un navigateur et a maintenant accès au portail d'applications pour une session de quatre heures, comme spécifié par la règle d'accès par défaut.
- 2 Au bout de 4 heures, l'utilisateur tente de lancer une application Web à laquelle la stratégie Application Web sensibles est appliquée.
- 3 Le service vérifie les règles de la stratégie et applique la stratégie avec la plage réseau TOUTES LES PLAGES, car la demande de l'utilisateur provient d'un navigateur Web et de la plage réseau TOUTES LES PLAGES.

L'utilisateur se connecte à l'aide de la méthode d'authentification RSA SecurID, mais la session vient d'expirer. L'utilisateur est redirigé pour une réauthentification. La réauthentification fournit à l'utilisateur une autre session de 4 heures et la possibilité de lancer l'application. Pendant les 4 heures suivantes, l'utilisateur peut continuer à lancer l'application sans devoir se réauthentifier.

Exemple 2 Stratégie spécifique à une application Web plus stricte

Pour qu'une règle plus stricte s'applique à des applications Web extra sensibles, vous pouvez avoir à vous authentifier de nouveau avec Secureld sur un périphérique après une heure. Voici un exemple de la mise en œuvre d'une règle d'accès de ce type de stratégie.

- 1 L'utilisateur se connecte depuis un réseau d'entreprise à l'aide de la méthode d'authentification par mot de passe.
L'utilisateur peut à présent accéder au portail d'applications pendant huit heures, comme indiqué dans l'exemple 1.
- 2 L'utilisateur tente immédiatement de lancer une application Web à laquelle la règle de stratégie Exemple 2 est appliquée, ce qui nécessite une authentification RSA SecurID.
- 3 L'utilisateur est redirigé vers un fournisseur d'identité qui fournit une authentification RSA SecurID.

- 4 Une fois que l'utilisateur s'est connecté, le service lance l'application et enregistre l'événement d'authentification.

L'utilisateur peut continuer à lancer cette application pendant au moins une heure, mais doit se réauthentifier au bout d'une heure, comme l'exige la règle de stratégie.

Gérer la stratégie d'accès de l'utilisateur

vRealize Automation est livré avec une stratégie d'accès de l'utilisateur par défaut que vous pouvez employer telle quelle ou modifier selon vos besoins afin de gérer l'accès des locataires aux applications.

vRealize Automation est livré avec une stratégie d'accès de l'utilisateur par défaut et vous ne pouvez pas ajouter de nouvelles stratégies. En revanche, vous pouvez modifier la stratégie existante afin d'ajouter des règles.

Prérequis

- Sélectionnez les fournisseurs d'identités adaptés à votre déploiement ou configurez-les. Reportez-vous à [Configurer une connexion de fournisseur d'identité tiers](#).
- Configurez les plages réseau adaptées à votre déploiement. Reportez-vous à [Ajout ou modification d'une plage réseau](#).
- Configurez les méthodes d'authentification adaptées à votre déploiement. Reportez-vous à [Intégration d'autres produits d'authentification de l'utilisateur à Directories Management](#).
- Si vous prévoyez de modifier la stratégie par défaut (pour contrôler globalement l'accès de l'utilisateur au service), configurez-la avant de créer une stratégie spécifique à une application Web.
- Ajoutez les applications Web au catalogue. Les applications Web doivent être répertoriées sur la page Catalogue avant de pouvoir ajouter une stratégie.
- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

- 1 Sélectionnez **Administration > Directories Management > Stratégies**.
- 2 Pour ajouter une nouvelle stratégie, cliquez sur **Modifier une stratégie**.
- 3 Ajoutez le nom et la description de la stratégie dans les zones de texte respectives.
- 4 Dans la section Appliquer à, cliquez sur **Sélectionner** et, sur la page qui s'affiche, sélectionnez les applications Web associées à cette stratégie.
- 5 Dans la section Règles de la stratégie, cliquez sur **+** pour ajouter une règle.

La page Ajouter une règle de stratégie s'affiche.

- a Sélectionnez la plage réseau pour appliquer cette règle.
- b Sélectionnez le type de périphérique pouvant accéder aux applications Web pour cette règle.
- c Sélectionnez les méthodes d'authentification à utiliser, dans l'ordre dans lequel elles doivent être appliquées.

- d Spécifiez le nombre d'heures pendant lesquelles une session d'application Web doit rester ouverte.
 - e Cliquez sur **Enregistrer**.
- 6 Configurez des règles supplémentaires si nécessaire.
- 7 Cliquez sur **Enregistrer**.

Configuration des connexions de fournisseur d'identité supplémentaires

Vous pouvez configurer des connexions de fournisseur d'identité supplémentaires si nécessaire afin de prendre en charge différents scénarios de gestion d'identité, y compris des fournisseurs d'identité intégrés supplémentaires et des fournisseurs d'identité tiers.

Vous pouvez créer trois types de connexions de fournisseur d'identité à l'aide de la gestion des annuaires.

- Créez une instance de fournisseur d'identité tiers - Utilisez cet élément pour créer une connexion vers un fournisseur d'identité tiers externe. Assurez-vous que vous avez bien suivi les étapes suivantes avant d'ajouter une instance de fournisseur d'identité tiers.
 - Vérifiez que les instances tierces sont conformes à la norme SAML 2.0 et que le service peut atteindre l'instance tierce.
 - Obtenez les informations sur les métadonnées tierces à ajouter lors de la configuration du fournisseur d'identité dans la console d'administration. Les informations de métadonnées que vous obtenez de l'instance tierce correspondent à l'URL d'accès aux métadonnées ou aux métadonnées proprement dites.
- Créer une instance de fournisseur d'identité Workspace - Lorsque vous activez un connecteur pour authentifier les utilisateurs lors de la configuration de la gestion des annuaires, un fournisseur d'identité Workspace est créé comme le fournisseur d'identité et l'authentification par mot de passe est activée. Vous pouvez configurer des fournisseurs d'identité Workspace supplémentaires derrière différents équilibres de charge.
- Créer un fournisseur d'identité intégré - Les fournisseurs d'identité intégrés utilisent les mécanismes de la gestion des annuaires internes pour prendre en charge l'authentification. Vous pouvez configurer des fournisseurs d'identité intégrés pour utiliser les méthodes d'authentification qui ne nécessitent pas l'utilisation d'un connecteur sur site. Lorsque vous configurez le fournisseur intégré, vous associez les méthodes d'authentification à utiliser avec le fournisseur.
- [Configurer une connexion de fournisseur d'identité tiers](#)
vRealize Automation est fourni avec une instance de connexion de fournisseur d'identité par défaut. Les utilisateurs peuvent souhaiter créer des connexions de fournisseur d'identité supplémentaires pour prendre en charge le provisionnement d'utilisateurs juste-à-temps ou d'autres configurations personnalisées.
- [Configurer des fournisseurs d'identité Workspace supplémentaires](#)
Lorsque vous configurez un connecteur de la gestion des annuaires afin d'authentifier des utilisateurs, un fournisseur d'identité Workspace est créé et l'authentification par mot de passe est activée.

- **Configurer une connexion de fournisseur d'identité intégré**

Vous pouvez configurer plusieurs fournisseurs d'identité intégrés et leur associer des méthodes d'authentification.

Configurer une connexion de fournisseur d'identité tiers

vRealize Automation est fourni avec une instance de connexion de fournisseur d'identité par défaut. Les utilisateurs peuvent souhaiter créer des connexions de fournisseur d'identité supplémentaires pour prendre en charge le provisionnement d'utilisateurs juste-à-temps ou d'autres configurations personnalisées.

vRealize Automation est fourni avec un fournisseur d'identité par défaut. Dans la plupart des cas, ce fournisseur suffit à satisfaire les besoins du consommateur. L'utilisation d'une solution d'entreprise existante pour la gestion des identités vous permet de configurer un fournisseur d'identité personnalisé pour rediriger les utilisateurs vers votre solution d'identité existante.

Lorsque vous utilisez un fournisseur d'identité personnalisé, la gestion des annuaires utilise des métadonnées SAML de ce fournisseur afin d'établir une relation de confiance avec le fournisseur. Une fois cette relation établie, la gestion des annuaires mappe les utilisateurs de l'assertion SAML à la liste des utilisateurs internes de vRealize Automation en fonction de l'ID de nom de sujet.

Prérequis

- Configurez les plages réseau que vous souhaitez rediriger vers cette instance de fournisseur d'identité à des fins d'authentification. Reportez-vous à [Ajout ou modification d'une plage réseau](#).
- Accédez au document sur les métadonnées tierces. Il peut s'agir de l'URL d'accès aux métadonnées ou des métadonnées proprement dites.
- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

- 1 Sélectionnez **Administration > Gestion des annuaires > Fournisseurs d'identité**.

Cette page affiche tous les fournisseurs d'identité configurés.

- 2 Cliquez sur **Ajouter un fournisseur d'identité**.

Un menu s'affiche avec les options Fournisseur d'identité.

- 3 Sélectionnez **Créer un IDP tiers**.

4 Entrez les informations appropriées pour configurer le fournisseur d'identité.

Option	Description
Nom du fournisseur d'identité	Entrez un nom pour cette instance de fournisseur d'identité.
Métadonnées SAML	<p>Ajoutez le document sur les métadonnées XML IdP tierces afin d'établir une relation d'approbation avec le fournisseur d'identité.</p> <ol style="list-style-type: none"> 1 Entrez l'URL des métadonnées SAML ou le contenu XML dans la zone de texte. 2 Cliquez sur Traiter les métadonnées IdP. Les formats NameID pris en charge par l'IdP sont extraits des métadonnées et ajoutés au tableau Format d'ID de nom. 3 Dans la colonne de valeurs ID de nom, sélectionnez l'attribut utilisateur dans le service à mapper aux formats d'ID affichés. Vous pouvez ajouter des formats d'ID de nom tiers et les mapper aux valeurs d'attribut utilisateur du service. 4 (Facultatif) Sélectionnez le format de la chaîne d'identificateur de réponse NameIDPolicy.
Utilisateurs	Sélectionnez les annuaires Directories Management des utilisateurs qui peuvent s'authentifier à l'aide de ce fournisseur d'identité.
Provisionnement d'utilisateurs juste-à-temps	<p>Sélectionnez les options appropriées pour prendre en charge le provisionnement juste-à-temps à l'aide d'un fournisseur d'identité tiers approprié.</p> <p>Entrez le Nom de l'annuaire à utiliser pour le provisionnement juste-à-temps.</p> <p>Entrez un ou plusieurs Domaines qui existent au sein du fournisseur d'identité externe que vous utiliserez pour le provisionnement juste-à-temps.</p>
Réseau	<p>Les plages réseau existantes configurées dans le service sont répertoriées.</p> <p>Sélectionnez les plages réseau des utilisateurs, en fonction de leurs adresses IP, que vous souhaitez rediriger vers cette instance de fournisseur d'identité à des fins d'authentification.</p>
Méthodes d'authentification	<p>Ajoutez les méthodes d'authentification prises en charge par le fournisseur d'identité tiers.</p> <p>Sélectionnez la classe de contexte d'authentification SAML qui prend en charge la méthode d'authentification.</p>
Certificat de signature SAML	Cliquez sur Métadonnées du fournisseur de services (SP) pour voir l'URL d'accès aux métadonnées du fournisseur de services SAML Directories Management. Copiez et enregistrez l'URL. Cette URL est configurée lorsque vous modifiez l'assertion SAML dans le fournisseur d'identité tiers pour mapper des utilisateurs Directories Management.
Nom d'hôte	Si le champ Nom d'hôte s'affiche, entrez le nom d'hôte vers lequel le fournisseur d'identité est redirigé pour authentification. Si vous utilisez un port non standard autre que 443, vous pouvez le définir avec le format Nom d'hôte:Port. Par exemple, myco.example.com:8443.

5 Cliquez sur **Ajouter**.

Suivant

- Copiez et enregistrez les métadonnées du fournisseur de service Directories Management qui sont nécessaires pour configurer l'instance de fournisseur d'identité tiers. Ces métadonnées sont disponibles dans la section Certificat de signature SAML de la page Fournisseur d'identité.
- Ajoutez la méthode d'authentification du fournisseur d'identité à la stratégie par défaut des services.

Consultez le guide *Configuration des ressources dans Directories Management* pour obtenir des informations sur l'ajout et la personnalisation des ressources que vous ajoutez au catalogue.

Configurer des fournisseurs d'identité Workspace supplémentaires

Lorsque vous configurez un connecteur de la gestion des annuaires afin d'authentifier des utilisateurs, un fournisseur d'identité Workspace est créé et l'authentification par mot de passe est activée.

Vous pouvez configurer des connecteurs supplémentaires pour travailler derrière plusieurs équilibres de charge. Lorsque votre déploiement inclut plusieurs équilibres de charge, vous pouvez configurer des fournisseurs d'identité Workspace supplémentaires pour l'authentification dans chaque configuration à équilibre de charge.

Procédure

- 1 Sélectionnez **Administration > Gestion des annuaires > Fournisseurs d'identité**.

Cette page affiche tous les fournisseurs d'identité configurés.

- 2 Cliquez sur **Ajouter un fournisseur d'identité**.

Un menu s'affiche avec les options Fournisseur d'identité.

- 3 Sélectionnez **Créer un nom de domaine complet Workspace**.

- 4 Entrez les informations appropriées pour configurer le fournisseur d'identité.

Option	Description
Nom du fournisseur d'identité	Entrez un nom pour cette instance du fournisseur d'identité intégré.
Utilisateurs	Sélectionnez les utilisateurs à authentifier. Les annuaires configurés sont répertoriés.
Utilisateurs	Sélectionnez le groupe d'utilisateurs qui peuvent s'authentifier à l'aide de ce fournisseur d'identité.
Réseau	Les plages réseau existantes configurées dans le service sont répertoriées. Sélectionnez la plage réseau des utilisateurs en fonction des adresses IP que vous souhaitez rediriger vers cette instance de fournisseur d'identité à des fins d'authentification.
Méthodes d'authentification	Les méthodes d'authentification qui sont configurées pour le service sont affichées. Cochez la case des méthodes d'authentification à associer à ce fournisseur d'identité. Pour la conformité des périphériques et le mot de passe, avec AirWatch et AirWatch Connector, assurez-vous que l'option est activée sur la page de configuration AirWatch.

- 5 Cliquez sur **Ajouter**.

Configurer une connexion de fournisseur d'identité intégré

Vous pouvez configurer plusieurs fournisseurs d'identité intégrés et leur associer des méthodes d'authentification.

Prérequis

Si vous utilisez l'authentification Kerberos intégré, téléchargez le certificat de l'émetteur KDC à utiliser dans la configuration AirWatch du profil de gestion du périphérique iOS.

Procédure

1 Sélectionnez **Administration > Gestion des annuaires > Fournisseurs d'identité**.

Cette page affiche tous les fournisseurs d'identité configurés.

2 Cliquez sur **Ajouter un fournisseur d'identité**.

Un menu s'affiche avec les options Fournisseur d'identité.

3 Sélectionnez **Créer une instance de fournisseur d'identité intégré**.

4 Entrez les informations appropriées pour configurer le fournisseur d'identité.

Option	Description
Nom du fournisseur d'identité	Entrez un nom pour cette instance du fournisseur d'identité intégré.
Utilisateurs	Sélectionnez les utilisateurs à authentifier. Les annuaires configurés sont répertoriés.
Réseau	Les plages réseau existantes configurées dans le service sont répertoriées. Sélectionnez la plage réseau des utilisateurs en fonction des adresses IP que vous souhaitez rediriger vers cette instance de fournisseur d'identité à des fins d'authentification.
Méthodes d'authentification	Les méthodes d'authentification qui sont configurées pour le service sont affichées. Cochez la case des méthodes d'authentification à associer à ce fournisseur d'identité. Pour la conformité des périphériques et le mot de passe, avec AirWatch et AirWatch Connector, assurez-vous que l'option appropriée est activée sur la page de configuration AirWatch.

5 Cliquez sur **Ajouter**.

Intégration d'autres produits d'authentification de l'utilisateur à Directories Management

Vous réalisez la configuration initiale de la fonctionnalité Directories Management à l'aide des connecteurs fournis avec votre infrastructure vRealize Automation existante. Ils vous permettent de créer une connexion Active Directory pour l'authentification et la gestion reposant sur l'ID d'utilisateur et le mot de passe. Mais vous pouvez également intégrer Directories Management à d'autres solutions d'authentification, telles que Kerberos ou RSA SecurID.

L'instance du fournisseur d'identité peut être l'instance du connecteur Directories Management, des instances de fournisseurs d'identité tiers ou une combinaison des deux.

L'instance de fournisseur d'identité que vous utilisez avec le service Directories Management crée une autorité fédératrice intégrée au réseau qui communique avec le service à l'aide d'assertions SAML 2.0.

Lors du déploiement initial du service Directories Management, le connecteur est le fournisseur d'identité initial pour le service. Votre infrastructure Active Directory existante est utilisée pour l'authentification et la gestion des utilisateurs.

Les méthodes d'authentification suivantes sont prises en charge. Vous configurez ces méthodes d'authentification à partir de la console d'administration.

Tableau 2-8. Types d'authentification de l'utilisateur pris en charge par Directories Management

Types d'authentification	Description
Mot de passe (déploiement sur site)	Sans configuration supplémentaire après la configuration d'Active Directory, Directories Management prend en charge l'authentification par mot de passe d'Active Directory. Cette méthode authentifie les utilisateurs avec Active Directory.
Kerberos pour postes de travail	L'authentification Kerberos fournit aux utilisateurs de domaine un accès à authentification unique à leur portail d'applications. Les utilisateurs n'ont pas besoin de se connecter de nouveau une fois qu'ils sont connectés au réseau.
Certificat (déploiement sur site)	L'authentification par certificat peut être configurée afin de permettre aux utilisateurs de s'authentifier avec des certificats sur leur poste de travail et périphériques mobiles ou d'utiliser un adaptateur de carte à puce pour l'authentification. L'authentification par certificat est basée sur ce que possède l'utilisateur et sur ce que la personne sait. Un certificat X.509 utilise la norme d'infrastructure de clé publique pour vérifier qu'une clé publique contenue dans le certificat appartient à l'utilisateur.
RSA SecurID (déploiement sur site)	Lorsque l'authentification RSA SecurID est configurée, Directories Management est configuré comme agent d'authentification sur le serveur RSA SecurID. L'authentification RSA SecurID nécessite l'utilisation d'un système d'authentification à jeton par les utilisateurs. RSA SecurID est une méthode d'authentification pour les utilisateurs qui accèdent à Directories Management depuis l'extérieur du réseau de l'entreprise.
RADIUS (déploiement sur site)	L'authentification RADIUS fournit des options d'authentification à deux facteurs. Vous configurez le serveur RADIUS qui est accessible par le service Directories Management. Lorsque des utilisateurs se connectent avec leur nom d'utilisateur et leur code secret, une demande d'accès est soumise au serveur RADIUS pour authentification.
RSA Adaptive Authentication (déploiement sur site)	L'authentification RSA offre une authentification multifactor plus forte que l'authentification par nom d'utilisateur et mot de passe avec Active Directory. Lorsque RSA Adaptive Authentication est activé, les indicateurs de risque spécifiés dans la stratégie de risque sont configurés dans l'application RSA Policy Management. La configuration du service Directories Management d'Adaptive Authentication est utilisée pour déterminer les invites d'authentification requises.
Mobile SSO (pour iOS)	L'authentification Mobile SSO pour iOS est utilisée pour l'authentification Single Sign-On pour les périphériques iOS gérés par AirWatch. L'authentification Mobile SSO (pour iOS) utilise un centre de distribution de clés (KDC) qui fait partie du service Directories Management. Vous devez initier le service KDC dans le service VMware Identity Manager avant de pouvoir activer cette méthode d'authentification.
Mobile SSO (pour Android)	L'authentification Mobile SSO pour Android est utilisée pour l'authentification Single Sign-On pour les périphériques Android gérés par AirWatch. Un service proxy est configuré entre le service Directories Management et AirWatch pour récupérer le certificat auprès d'AirWatch à des fins d'authentification.
Mot de passe (AirWatch Connector)	AirWatch Cloud Connector peut être intégré au service Directories Management pour l'authentification par mot de passe utilisateur. Vous configurez le service Directories Management pour synchroniser des utilisateurs à partir de l'annuaire AirWatch.

Les utilisateurs sont authentifiés en fonction des méthodes d'authentification, des règles de stratégie d'accès par défaut, des plages réseau et de l'instance du fournisseur d'identité que vous configurez. Une fois les méthodes d'authentification configurées, vous créez des règles de stratégie d'accès qui spécifient les méthodes d'authentification à utiliser par type de périphérique.

Configuration de SecurID pour Directories Management

Lorsque vous configurez le serveur RSA SecurID, vous devez ajouter les informations sur le service du Directories Management en tant qu'agent d'authentification sur le serveur RSA SecurID, et configurer les informations du serveur RSA SecurID sur le service du Directories Management.

Lorsque vous configurez SecurID pour offrir une sécurité supplémentaire, vous devez vérifier que votre réseau est correctement configuré pour votre déploiement de Directories Management. Pour SecurID en particulier, assurez-vous que le port adéquat est ouvert afin de permettre à SecurID d'authentifier les utilisateurs hors de votre réseau.

Après avoir exécuté l'assistant Configuration du Directories Management et configuré votre connexion à Active Directory, vous disposez des informations nécessaires à la préparation du serveur RSA SecurID. Après avoir préparé le serveur RSA SecurID de Directories Management, activez SecurID dans la console d'administration.

■ Préparer le serveur RSA SecurID

Le serveur RSA SecurID doit être configuré avec des informations sur le dispositif Directories Management en tant qu'agent d'authentification. Les informations requises correspondent au nom d'hôte et aux adresses IP des interfaces réseau.

■ Configurer l'authentification RSA SecurID

Après avoir configuré Directories Management en tant qu'agent d'authentification dans le serveur RSA SecurID, ajoutez les informations de configuration du RSA SecurID au connecteur.

Préparer le serveur RSA SecurID

Le serveur RSA SecurID doit être configuré avec des informations sur le dispositif Directories Management en tant qu'agent d'authentification. Les informations requises correspondent au nom d'hôte et aux adresses IP des interfaces réseau.

Prérequis

- Vérifiez que l'une des versions suivantes de RSA Authentication Manager est installée et fonctionne sur le réseau d'entreprise : RSA AM 6.1.2, 7.1 SP2 et versions ultérieures, ainsi que 8.0 et versions ultérieures. Le serveur Directories Management utilise AuthSDK_Java_v8.1.1.312.06_03_11_03_16_51 (Agent API 8.1 SP1), qui prend en charge uniquement les versions précédentes de RSA Authentication Manager (serveur RSA SecurID). Pour obtenir des informations sur l'installation et la configuration de RSA Authentication Manager (serveur RSA SecurID), consultez la documentation de RSA.

Procédure

- 1 Sur une version prise en charge du serveur RSA SecurID, ajoutez le connecteur Directories Management en tant qu'agent d'authentification. Entrez les informations suivantes.

Option	Description
nom d'hôte	Le nom d'hôte de Directories Management.
Adresse IP	L'adresse IP de Directories Management.
Adresse IP alternative	Si le trafic provenant du connecteur traverse un périphérique NAT (Network Address Translation) pour atteindre le serveur RSA SecurID, entrez l'adresse IP privée du dispositif.

- 2 Téléchargez le fichier de configuration compressé et extrayez le fichier `sdconf.rec`.
Préparez-vous à charger ce fichier ultérieurement lorsque vous configurez RSA SecurID dans Directories Management.

Suivant

Accédez à la console d'administration et, dans les pages Configuration de l'onglet Gestion des identités et des accès, sélectionnez le connecteur et la page Adaptateurs d'authentification pour configurer SecurID.

Configurer l'authentification RSA SecurID

Après avoir configuré Directories Management en tant qu'agent d'authentification dans le serveur RSA SecurID, ajoutez les informations de configuration du RSA SecurID au connecteur.

Prérequis

- Vérifiez que RSA Authentication Manager (serveur RSA SecurID) est installé et correctement configuré.
- Téléchargez le fichier compressé depuis le serveur RSA SecurID et extrayez le fichier de configuration du serveur.

Procédure

- 1 En tant qu'administrateur de locataire, accédez à **Administration > Directories Management > Connecteurs**.
- 2 Sur la page Connecteurs, sélectionnez le lien Travailleur correspondant au connecteur qui est configuré avec RSA SecurID.
- 3 Cliquez sur **Adaptateurs d'authentification**, puis cliquez sur **SecurIDIdpAdapter**.
Vous serez redirigé vers la page de connexion du gestionnaire d'identité.
- 4 Sur la ligne SecurIDIdpAdapter de la page Adaptateurs d'authentification, cliquez sur **Modifier**.
- 5 Configurez la page Adaptateur d'authentification SecurID.

Les informations utilisées et les fichiers générés sur le serveur RSA SecurID sont nécessaires lors de la configuration de la page SecurID.

Option	Action
Nom	Un nom est requis. Le nom par défaut est SecurIDIdpAdapter. Vous pouvez modifier ce paramètre.
Activer SecurID	Cochez cette case pour activer l'authentification SecurID.
Nombre de tentatives d'authentification autorisées	Entrez le nombre maximal d'échecs de tentatives de connexion à l'aide du jeton RSA SecurID. La valeur par défaut est de cinq tentatives.
Adresse du connecteur	Entrez l'adresse IP de l'instance de connecteur. La valeur que vous entrez doit correspondre à la valeur que vous avez utilisée lorsque vous avez ajouté le dispositif du connecteur en tant qu'agent d'authentification du serveur RSA SecurID. Si votre serveur RSA SecurID dispose d'une valeur assignée à l'invite Adresse IP alternative, entrez cette valeur comme adresse IP du connecteur. Si aucune adresse IP alternative n'est attribuée, entrez la valeur attribuée à l'invite de l'adresse IP.
Adresse IP de l'agent	Entrez la valeur assignée à l'invite Adresse IP sur le serveur RSA SecurID.
Configuration du serveur	Chargez le fichier de configuration du serveur RSA SecurID. Vous devez d'abord télécharger le fichier compressé auprès du serveur RSA SecurID, puis extraire le fichier de configuration du serveur qui est appelé par défaut <code>sdconf.rec</code> .
Nœud secret	Laisser vide le champ nœud secret permet à celui-ci de se générer lui-même. Nous vous recommandons d'effacer le fichier du secret du nœud du serveur RSA SecurID et de ne pas charger volontairement le fichier du secret du nœud. Assurez-vous que le fichier du nœud secret sur le serveur RSA SecurID et sur l'instance du connecteur de serveur correspondent toujours. Si vous modifiez le nœud secret à un emplacement, modifiez-le sur l'autre emplacement.

6 Cliquez sur **Enregistrer**.

Suivant

Ajoutez la méthode d'authentification à la stratégie d'accès par défaut. Accédez à **Administration > Directories Management > Stratégies**. Pour modifier les règles de stratégie par défaut et y ajouter la méthode d'authentification SecurID dans le bon ordre d'authentification, cliquez sur **Modifier la stratégie par défaut**.

Configuration de RADIUS pour Directories Management

Vous pouvez configurer Directories Management pour que les utilisateurs soient obligés d'utiliser l'authentification RADIUS (Remote Authentication Dial-In User Service). Vous configurez les informations du serveur RADIUS sur le service Directories Management.

Le support RADIUS offre une large gamme d'options alternatives d'authentification à jeton à deux facteurs. Puisque ces solutions d'authentification à deux facteurs, telles que RADIUS, fonctionnent avec les gestionnaires d'authentification installés sur des serveurs distincts, configurez le serveur RADIUS et mettez-le à disposition du service du gestionnaire d'identité.

Lorsque les utilisateurs se connectent à leur portail My Apps et que l'authentification RADIUS est activée, une boîte de dialogue de connexion spéciale apparaît dans le navigateur. Les utilisateurs entrent leur nom d'utilisateur et leur code secret d'authentification RADIUS dans la boîte de dialogue de connexion. Si le serveur RADIUS émet une stimulation d'accès, le service du gestionnaire d'identité ouvre une boîte de dialogue qui invite à entrer un second code secret. Le support actuel des challenges RADIUS est limité à la demande de saisie de texte.

Une fois que l'utilisateur a entré ses informations d'identification dans la boîte de dialogue, le serveur RADIUS peut envoyer un SMS ou un e-mail, ou du texte à l'aide d'un autre mécanisme hors bande sur le téléphone portable de l'utilisateur avec un code. L'utilisateur peut entrer ce texte et le code dans la boîte de dialogue de connexion pour terminer l'authentification.

Si le serveur RADIUS permet d'importer des utilisateurs depuis Active Directory, les utilisateurs finaux peuvent d'abord être invités à fournir des informations d'identification Active Directory avant d'être invités à fournir un nom d'utilisateur et un code secret d'authentification RADIUS.

Préparer le serveur RADIUS

Configurez le serveur RADIUS, puis définissez ses paramètres pour qu'il accepte les demandes RADIUS émises par le service Directories Management.

Pour plus d'informations sur la configuration du serveur RADIUS, consultez les guides de configuration du fournisseur RADIUS. Notez les informations de votre configuration RADIUS car vous en avez besoin lorsque vous configurez RADIUS dans le service. Pour afficher le type d'informations RADIUS requises pour configurer Directories Management, reportez-vous à [Configurer l'authentification RADIUS dans Directories Management](#).

Vous pouvez configurer un serveur d'authentification Radius secondaire afin de l'utiliser pour la haute disponibilité. Si le serveur RADIUS principal ne répond pas dans le délai d'attente du serveur configuré pour l'authentification RADIUS, la demande est routée vers le serveur secondaire. Lorsque le serveur principal ne répond pas, le serveur secondaire reçoit toutes les futures demandes d'authentification.

Configurer l'authentification RADIUS dans Directories Management

Activez le logiciel RADIUS sur un serveur du gestionnaire d'authentification. Pour l'authentification RADIUS, suivez la documentation de configuration du fournisseur.

Prérequis

Installez et configurez le logiciel RADIUS sur un serveur de gestion de l'authentification. Pour l'authentification RADIUS, suivez la documentation de configuration du fournisseur.

Vous devez connaître les informations suivantes sur le serveur RADIUS pour configurer RADIUS sur le service.

- Adresse IP ou nom DNS du serveur RADIUS.
- Numéros de port d'authentification. En général, le port d'authentification est le port 1812.
- Type d'authentification. Les types d'authentification incluent PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), MSCHAP1, MSCHAP2 (Microsoft Challenge Handshake Authentication Protocol, versions 1 et 2).

- Code secret partagé RADIUS utilisé pour le chiffrement et le déchiffrement dans les messages de protocole RADIUS.
- Valeurs de délai d'expiration et de nouvelle tentative spécifiques nécessaires pour l'authentification RADIUS.
- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

- 1 Sélectionnez **Administration > Directories Management > Connecteurs**.
- 2 Sur la page Connecteurs, sélectionnez le lien Travailleur correspondant au connecteur qui est configuré pour l'authentification RADIUS.
- 3 Cliquez sur **Adaptateurs d'authentification**, puis cliquez sur **RadiusAuthAdapter**.
Vous serez redirigé vers la page de connexion du gestionnaire d'identité.
- 4 Cliquez sur **Modifier** pour configurer ces champs sur la page Adaptateur d'authentification.

Option	Action
Nom	Un nom est requis. Le nom par défaut est RadiusAuthAdapter. Vous pouvez modifier ce paramètre.
Activer l'adaptateur Radius	Cochez cette case pour activer l'authentification RADIUS.
Nombre de tentatives d'authentification autorisées	Entrez le nombre maximum de tentatives de connexion échouées lorsque vous utilisez RADIUS pour vous connecter. La valeur par défaut est de cinq tentatives.
Nombre de tentatives pour le serveur Radius	Spécifiez le nombre total de nouvelles tentatives. Si le serveur principal ne répond pas, le service attend l'heure configurée avant de réessayer.
Nom d'hôte/adresse du serveur Radius	Entrez le nom de l'hôte ou l'adresse IP du serveur RADIUS.
Port d'authentification	Entrez le numéro de port d'authentification Radius. En général, il s'agit du port 1812.
Port de gestion	Entrez 0 pour le numéro de port. Le port de gestion n'est pas utilisé actuellement.
Type d'authentification	Entrez le protocole d'authentification pris en charge par le serveur RADIUS. PAP, CHAP, MSCHAP1 ou MSCHAP2.
Code secret partagé	Entrez le code secret partagé utilisé entre le serveur RADIUS et le service VMware Identity Manager.

Option	Action
Délai d'attente du serveur en secondes	Entrez le délai d'attente du serveur RADIUS en secondes, après lequel une nouvelle tentative est envoyée si le serveur RADIUS ne répond pas.
Préfixe du domaine	(Facultatif) L'emplacement du compte d'utilisateur est appelé le domaine. Si vous spécifiez une chaîne de préfixe du domaine, la chaîne est placée au début du nom d'utilisateur lorsque le nom est envoyé au serveur RADIUS. Par exemple, si le nom d'utilisateur entré est jdoe et que le préfixe de domaine DOMAIN-A\ est spécifié, le nom d'utilisateur DOMAIN-A\jdoe est envoyé au serveur RADIUS. Si vous ne configurez pas ces champs, seul le nom d'utilisateur qui est entré est envoyé.
Suffixe du domaine	(Facultatif) Si vous spécifiez un suffixe du domaine, la chaîne est placée à la fin du nom d'utilisateur. Par exemple, si le suffixe est @myco.com, le nom d'utilisateur jdoe@myco.com est envoyé au serveur RADIUS.
Conseil pour la phrase secrète de la page de connexion	Entrez la chaîne de texte à afficher dans le message sur la page de connexion utilisateur pour demander aux utilisateurs d'entrer le bon code secret Radius. Par exemple, si ce champ est configuré avec Mot de passe AD en premier, puis code secret SMS , le message sur la page de connexion serait Entrez votre mot de passe AD en premier, puis le code secret SMS . La chaîne de texte par défaut est RADIUS Passcode .

5 Vous pouvez activer un serveur RADIUS secondaire pour une haute disponibilité.

Configurez le serveur secondaire comme décrit à l'étape 4.

6 Cliquez sur **Enregistrer**.

Suivant

Ajoutez la méthode d'authentification RADIUS à la stratégie d'accès par défaut. Sélectionnez **Administration > Directories Management > Stratégies**. Pour modifier les règles de stratégie par défaut et y ajouter la méthode d'authentification RADIUS dans le bon ordre d'authentification, cliquez ensuite sur **Modifier la stratégie par défaut**.

Configuration d'un certificat ou d'un adaptateur de carte à puce pour Directories Management

Vous pouvez configurer l'authentification par certificat x509 afin de permettre aux utilisateurs de s'authentifier avec des certificats sur leur poste de travail et périphériques mobiles ou d'utiliser un adaptateur de carte à puce pour l'authentification. L'authentification par certificat est basée sur ce que possède l'utilisateur (la clé privée ou la carte à puce) et sur ce que la personne sait (le mot de passe de la clé privée ou le code PIN de la carte à puce). Un certificat X.509 utilise la norme d'infrastructure de clé publique (KPI) pour vérifier qu'une clé publique contenue dans le certificat appartient à l'utilisateur. Pour l'authentification par carte à puce, les utilisateurs connectent la carte à puce à l'ordinateur et saisissent un code PIN.

Les certificats des cartes à puce sont copiés dans le magasin de certificats local de l'ordinateur de l'utilisateur. Les certificats du magasin de certificats local sont disponibles pour tous les navigateurs exécutés sur l'ordinateur de cet utilisateur, avec certaines exceptions, et sont ainsi disponibles pour l'instance de Directories Management dans ce navigateur.

- **Utilisation du nom de l'utilisateur principal pour l'authentification par certificat**

Vous pouvez utiliser le mappage de certificat dans Active Directory. Les connexions par certificat et par carte à puce utilisent le nom de l'utilisateur principal (UPN) d'Active Directory pour valider les comptes d'utilisateur. Les comptes d'utilisateurs Active Directory qui essaient de s'authentifier dans le service Directories Management doivent disposer d'un UPN valide qui correspond à l'UPN du certificat.

- **Autorité de certification requise pour l'authentification**

Pour activer la connexion à l'aide de l'authentification par certificat, des certificats racine et intermédiaires doivent être chargés dans le Directories Management.

- **Utilisation du contrôle de la révocation des certificats**

Vous pouvez configurer le contrôle de la révocation des certificats pour empêcher les utilisateurs dont les certificats d'utilisateur sont révoqués de s'authentifier. Les certificats sont souvent révoqués lorsqu'un utilisateur quitte une organisation, perd une carte à puce ou change de service.

- **Configurer l'authentification du certificat dans la gestion des annuaires**

Activez et configurez l'authentification du certificat à partir de la fonctionnalité de la gestion des annuaires de la console d'administration vRealize Automation.

Utilisation du nom de l'utilisateur principal pour l'authentification par certificat

Vous pouvez utiliser le mappage de certificat dans Active Directory. Les connexions par certificat et par carte à puce utilisent le nom de l'utilisateur principal (UPN) d'Active Directory pour valider les comptes d'utilisateur. Les comptes d'utilisateurs Active Directory qui essaient de s'authentifier dans le service Directories Management doivent disposer d'un UPN valide qui correspond à l'UPN du certificat.

Vous pouvez configurer le Directories Management pour utiliser une adresse e-mail afin de valider le compte d'utilisateur si l'UPN n'existe pas dans le certificat.

Vous pouvez également activer un type d'UPN alternatif à utiliser.

Autorité de certification requise pour l'authentification

Pour activer la connexion à l'aide de l'authentification par certificat, des certificats racine et intermédiaires doivent être chargés dans le Directories Management.

Les certificats sont copiés dans le magasin de certificats local de l'ordinateur de l'utilisateur. Les certificats du magasin de certificats local sont disponibles pour tous les navigateurs exécutés sur l'ordinateur de cet utilisateur, avec certaines exceptions, et sont ainsi disponibles pour l'instance de Directories Management dans ce navigateur.

Pour l'authentification par carte à puce, lorsqu'un utilisateur initie une connexion sur une instance de Directories Management, le service Directories Management envoie une liste d'autorités de certification (CA) approuvées au navigateur. Le navigateur compare la liste des CA approuvées aux certificats d'utilisateur disponibles, sélectionne un certificat adapté, puis demande à l'utilisateur de saisir le code PIN d'une carte à puce. Si plusieurs certificats d'utilisateur valides sont disponibles, le navigateur demande à l'utilisateur de sélectionner un certificat.

Si un utilisateur ne peut pas s'authentifier, les autorités de certification racine et intermédiaire sont peut-être mal configurées, ou le service n'a peut-être pas été redémarré après le téléchargement des autorités de certification racine et intermédiaire sur le serveur. Dans ces situations, le navigateur ne peut pas afficher les certificats installés, l'utilisateur ne peut pas sélectionner le certificat correct, ce qui fait échouer l'authentification par certificat.

Utilisation du contrôle de la révocation des certificats

Vous pouvez configurer le contrôle de la révocation des certificats pour empêcher les utilisateurs dont les certificats d'utilisateur sont révoqués de s'authentifier. Les certificats sont souvent révoqués lorsqu'un utilisateur quitte une organisation, perd une carte à puce ou change de service.

Le contrôle de la révocation des certificats à l'aide de listes de révocation de certificats (CRL) et du protocole OCSP est pris en charge. Une CRL est une liste de certificats révoqués publiée par l'autorité de certification ayant émis les certificats. OCSP est un protocole de validation des certificats utilisé pour obtenir le statut de révocation d'un certificat.

Vous pouvez configurer le contrôle de la révocation des certificats sur la page Connecteurs > Adaptateurs d'authentification > CertificateAuthAdapter de la console d'administration lorsque vous configurez l'authentification par certificat.

Il est possible de configurer la CRL et OCSP en configurant le même adaptateur d'authentification par certificat. Lorsque vous configurez les deux types de contrôle de révocation des certificats et que la case Utiliser la CRL en cas de défaillance d'OCSP est cochée, OCSP est contrôlé en premier et, s'il échoue, le contrôle de la révocation est effectué par la CRL. Le contrôle de la révocation ne revient pas à OCSP en cas d'échec de la CRL.

Connexion avec le contrôle de la CRL

Lorsque la révocation des certificats est autorisée, le serveur Directories Management lit une CRL pour déterminer l'état de révocation d'un certificat d'utilisateur.

Si un certificat est révoqué, l'authentification par certificat échoue.

Connexion avec le contrôle de certificat OCSP

Lorsque vous configurez le contrôle de la révocation par le protocole OCSP, Directories Management envoie une demande à un répondeur OCSP pour déterminer le statut de révocation d'un certificat d'utilisateur spécifique. Le serveur Directories Management utilise le certificat de signature OCSP pour vérifier l'authenticité des réponses reçues de la part du répondeur OCSP.

Si le certificat est révoqué, l'authentification échoue.

Il est possible de configurer l'authentification pour basculer vers le contrôle par CRL si aucune réponse n'est reçue de la part du répondeur OCSP ou si la réponse n'est pas valide.

Configurer l'authentification du certificat dans la gestion des annuaires

Activez et configurez l'authentification du certificat à partir de la fonctionnalité de la gestion des annuaires de la console d'administration vRealize Automation.

Prérequis

- Obtenez les certificats racines et intermédiaires auprès de l'autorité de certification ayant signé les certificats présentés par vos utilisateurs.
- (Facultatif) Une liste des identificateurs d'objets (OID) des stratégies de certificat valides pour l'authentification par certificat.
- Pour le contrôle de la révocation, l'emplacement du fichier du CRL et l'URL du serveur OCSP.
- (Facultatif) L'emplacement du fichier de la signature du certificat de la réponse OCSP.
- Le contenu du formulaire de consentement, si un tel formulaire est activé et doit s'afficher avant l'authentification.

Procédure

- 1 En tant qu'administrateur de locataire, accédez à **Administration > Gestion des annuaires > Connecteurs**.
- 2 Sur la page Connecteurs, sélectionnez le lien Travailleur correspondant au connecteur qui est configuré.
- 3 Cliquez sur **Adaptateurs d'authentification**, puis cliquez sur **CertificateAuthAdapter**.
Vous serez redirigé vers la page de connexion du gestionnaire d'identité.
- 4 Dans la ligne CertificateAuthAdapter, cliquez sur **Modifier**.
- 5 Configurez la page Adaptateur d'authentification par certificat.

Remarque Les champs obligatoires sont indiqués par un astérisque. Tous les autres champs sont facultatifs.

Option	Description
*Nom	Un nom est requis. Le nom par défaut est CertificateAuthAdapter. Vous pouvez modifier ce nom.
Activer l'adaptateur de certificat	Cochez la case pour permettre l'authentification par certificat.
*Certificats d'autorité de certification racine et intermédiaire	Sélectionnez les fichiers de certificat à télécharger. Il est possible de sélectionner plusieurs certificats d'autorité de certification racine et intermédiaire qui utilisent l'encodage DER ou PEM.
Certificats d'autorité de certification téléchargés	<p>Les fichiers de certificat téléchargés sont répertoriés dans la section Certificats d'autorité de certification téléchargés du formulaire.</p> <p>Vous devez redémarrer le service pour que les nouveaux certificats soient disponibles.</p> <p>Cliquez sur Redémarrer le service Web pour redémarrer le service et ajouter les certificats au service approuvé.</p> <p>Remarque Le redémarrage du service n'active pas l'authentification par certificat. Une fois le service redémarré, continuez la configuration de cette page. Cliquez sur Enregistrer à la fin de la page active l'authentification par certificat sur le service.</p>

Option	Description
Utiliser une adresse e-mail s'il n'existe pas d'UPN dans le certificat	Si le nom principal de l'utilisateur (UPN) n'existe pas dans le certificat, cochez cette case pour utiliser l'attribut emailAddress comme extension Autre nom de l'objet afin de valider des comptes d'utilisateur.
Stratégies de certificat acceptées	Créez une liste d'identificateurs d'objet qui sont acceptés dans les extensions de stratégie de certificat. Entrez les numéros d'ID d'objet (OID) pour la stratégie d'émission de certificat. Cliquez sur Ajouter une autre valeur pour ajouter des OID supplémentaires.
Activer la révocation de certificat	Cochez cette case pour permettre le contrôle de la révocation des certificats. Cela empêche les utilisateurs avec des certificats d'utilisateur révoqués de s'authentifier.
Utiliser la CRL des certificats	Cochez cette case pour utiliser la liste de révocation de certificats (CRL) publiée par l'autorité de certification qui a émis les certificats afin de valider le statut d'un certificat, révoqué ou non révoqué.
Emplacement de la CRL	Entrez le chemin d'accès au fichier de serveur ou local depuis lequel la CRL peut être récupérée.
Autoriser la révocation OCSP	Cochez la case pour utiliser le protocole de validation des certificats OCSP (Online Certificate Status Protocol) afin d'obtenir le statut de révocation d'un certificat.
Utiliser la CRL en cas de défaillance du protocole	Si vous configurez une CRL et OCSP, vous pouvez cocher cette case pour basculer vers l'utilisation de la CRL si le contrôle OCSP n'est pas disponible.
Envoi de nonce OCSP	Cochez cette case si vous souhaitez que l'identificateur unique de la requête OCSP soit envoyée dans la réponse.
URL d'OCSP	Si vous avez activé la révocation OCSP, entrez l'adresse de serveur OCSP pour le contrôle de la révocation.
Certificat de la signature du répondeur OCSP	Entrez le chemin d'accès au certificat OCSP du répondeur, <i>/path/to/file.cer</i> .
Activer le formulaire de consentement avant l'authentification	Cochez cette case pour inclure une page du formulaire de consentement qui s'affiche avant que les utilisateurs se connectent à leur portail My Apps à l'aide de l'authentification par certificat.
Contenu du formulaire de consentement	Saisissez le texte qui s'affiche sur le formulaire de consentement dans cette zone de texte.

6 Cliquez sur **Enregistrer**.

Suivant

- Ajoutez la méthode d'authentification du certificat à la stratégie d'accès par défaut. Pour ce faire, accédez à **Administration > Gestion des annuaires > Stratégies**. Pour modifier les règles de la stratégie par défaut, y ajouter l'authentification du certificat et faire de cette méthode la première méthode d'authentification de la stratégie par défaut, cliquez sur **Modifier la stratégie par défaut**. Le certificat doit être la première méthode d'authentification répertoriée dans la règle de stratégie, sinon l'authentification par certificat échoue.

- Lorsque l'authentification par certificat est configurée et que le dispositif de service est configuré derrière un équilibrage de charge, assurez-vous que le connector Directories Management est configuré avec un passe-système SSL au niveau de l'équilibrage de charge et qu'il n'est pas configuré pour mettre fin à SSL au niveau de l'équilibrage de charge. Cette configuration permet de s'assurer que la négociation SSL a lieu entre le connecteur et le client afin de transmettre le certificat au connecteur.

Configuration d'une instance de fournisseur d'identité tiers pour authentifier des utilisateurs

Vous pouvez configurer un fournisseur d'identité tiers pour authentifier des utilisateurs dans le service Directories Management.

Effectuez les tâches suivantes avant d'utiliser la console d'administration pour ajouter l'instance de fournisseur d'identité tiers.

- Vérifiez que les instances tierces sont conformes à la norme SAML 2.0 et que le service peut atteindre l'instance tierce.
- Obtenez les informations sur les métadonnées tierces à ajouter lors de la configuration du fournisseur d'identité dans la console d'administration. Les informations de métadonnées que vous obtenez de l'instance tierce correspondent à l'URL d'accès aux métadonnées ou aux métadonnées proprement dites.

Configurer une connexion de fournisseur d'identité tiers

vRealize Automation est fourni avec une instance de connexion de fournisseur d'identité par défaut. Les utilisateurs peuvent souhaiter créer des connexions de fournisseur d'identité supplémentaires pour prendre en charge le provisionnement d'utilisateurs juste-à-temps ou d'autres configurations personnalisées.

vRealize Automation est fourni avec un fournisseur d'identité par défaut. Dans la plupart des cas, ce fournisseur suffit à satisfaire les besoins du consommateur. L'utilisation d'une solution d'entreprise existante pour la gestion des identités vous permet de configurer un fournisseur d'identité personnalisé pour rediriger les utilisateurs vers votre solution d'identité existante.

Lorsque vous utilisez un fournisseur d'identité personnalisé, la gestion des annuaires utilise des métadonnées SAML de ce fournisseur afin d'établir une relation de confiance avec le fournisseur. Une fois cette relation établie, la gestion des annuaires mappe les utilisateurs de l'assertion SAML à la liste des utilisateurs internes de vRealize Automation en fonction de l'ID de nom de sujet.

Prérequis

- Configurez les plages réseau que vous souhaitez rediriger vers cette instance de fournisseur d'identité à des fins d'authentification. Reportez-vous à [Ajout ou modification d'une plage réseau](#).
- Accédez au document sur les métadonnées tierces. Il peut s'agir de l'URL d'accès aux métadonnées ou des métadonnées proprement dites.
- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

1 Sélectionnez **Administration > Gestion des annuaires > Fournisseurs d'identité**.

Cette page affiche tous les fournisseurs d'identité configurés.

2 Cliquez sur **Ajouter un fournisseur d'identité**.

Un menu s'affiche avec les options Fournisseur d'identité.

3 Sélectionnez **Créer un IDP tiers**.

4 Entrez les informations appropriées pour configurer le fournisseur d'identité.

Option	Description
Nom du fournisseur d'identité	Entrez un nom pour cette instance de fournisseur d'identité.
Métadonnées SAML	<p>Ajoutez le document sur les métadonnées XML IdP tierces afin d'établir une relation d'approbation avec le fournisseur d'identité.</p> <ol style="list-style-type: none"> Entrez l'URL des métadonnées SAML ou le contenu XML dans la zone de texte. Cliquez sur Traiter les métadonnées IdP. Les formats NameID pris en charge par l'IdP sont extraits des métadonnées et ajoutés au tableau Format d'ID de nom. Dans la colonne de valeurs ID de nom, sélectionnez l'attribut utilisateur dans le service à mapper aux formats d'ID affichés. Vous pouvez ajouter des formats d'ID de nom tiers et les mapper aux valeurs d'attribut utilisateur du service. (Facultatif) Sélectionnez le format de la chaîne d'identificateur de réponse NameIDPolicy.
Utilisateurs	Sélectionnez les annuaires Directories Management des utilisateurs qui peuvent s'authentifier à l'aide de ce fournisseur d'identité.
Provisionnement d'utilisateurs juste-à-temps	<p>Sélectionnez les options appropriées pour prendre en charge le provisionnement juste-à-temps à l'aide d'un fournisseur d'identité tiers approprié.</p> <p>Entrez le Nom de l'annuaire à utiliser pour le provisionnement juste-à-temps.</p> <p>Entrez un ou plusieurs Domaines qui existent au sein du fournisseur d'identité externe que vous utiliserez pour le provisionnement juste-à-temps.</p>
Réseau	<p>Les plages réseau existantes configurées dans le service sont répertoriées.</p> <p>Sélectionnez les plages réseau des utilisateurs, en fonction de leurs adresses IP, que vous souhaitez rediriger vers cette instance de fournisseur d'identité à des fins d'authentification.</p>
Méthodes d'authentification	<p>Ajoutez les méthodes d'authentification prises en charge par le fournisseur d'identité tiers.</p> <p>Sélectionnez la classe de contexte d'authentification SAML qui prend en charge la méthode d'authentification.</p>
Certificat de signature SAML	Cliquez sur Métadonnées du fournisseur de services (SP) pour voir l'URL d'accès aux métadonnées du fournisseur de services SAML Directories Management. Copiez et enregistrez l'URL. Cette URL est configurée lorsque vous modifiez l'assertion SAML dans le fournisseur d'identité tiers pour mapper des utilisateurs Directories Management.
Nom d'hôte	Si le champ Nom d'hôte s'affiche, entrez le nom d'hôte vers lequel le fournisseur d'identité est redirigé pour authentification. Si vous utilisez un port non standard autre que 443, vous pouvez le définir avec le format Nom d'hôte:Port. Par exemple, myco.example.com:8443.

5 Cliquez sur **Ajouter**.

Suivant

- Copiez et enregistrez les métadonnées du fournisseur de service Directories Management qui sont nécessaires pour configurer l'instance de fournisseur d'identité tiers. Ces métadonnées sont disponibles dans la section Certificat de signature SAML de la page Fournisseur d'identité.
- Ajoutez la méthode d'authentification du fournisseur d'identité à la stratégie par défaut des services.

Consultez le guide *Configuration des ressources dans Directories Management* pour obtenir des informations sur l'ajout et la personnalisation des ressources que vous ajoutez au catalogue.

Gestion des méthodes d'authentification à appliquer aux utilisateurs

Le service Directories Management tente d'authentifier les utilisateurs selon les méthodes d'authentification, la stratégie d'accès par défaut, les plages réseau et les instances de fournisseurs d'identité que vous configurez.

Lorsque des utilisateurs tentent de se connecter, le service évalue les règles de stratégie par défaut pour déterminer la règle de la stratégie à appliquer. Les méthodes d'authentification sont appliquées dans l'ordre où elles sont répertoriées dans la règle. La première instance de fournisseur d'identité qui répond aux exigences relatives à la méthode d'authentification et à la plage réseau de la règle est sélectionnée, et la demande d'authentification de l'utilisateur est transmise à l'instance de fournisseur d'identité à des fins d'authentification. Si l'authentification échoue, la méthode d'authentification suivante configurée dans la règle est appliquée.

Vous pouvez ajouter des règles qui spécifient les méthodes d'authentification à utiliser par type de périphérique ou par type de périphérique et à partir d'une plage réseau spécifique. Par exemple, vous pouvez configurer une règle exigeant que les utilisateurs se connectent à l'aide de périphériques iOS à partir d'un réseau spécifique pour s'authentifier avec RSA SecurID et une autre règle qui spécifie que tous les types de périphérique se connectent à partir de l'adresse IP du réseau interne pour s'authentifier avec leur mot de passe.

Ajout ou modification d'une plage réseau

Vous pouvez gérer les plages réseau afin de définir les adresses IP à partir desquelles les utilisateurs peuvent se connecter via un lien Active Directory. Vous ajoutez les plages réseau que vous créez à des instances de fournisseurs d'identité spécifiques et pour accéder à des règles de stratégie.

Définissez les plages réseau pour votre déploiement de Directories Management en fonction de la topologie du réseau.

Une plage réseau, appelée TOUTES LES PLAGES, est créée comme plage par défaut. Cette plage réseau comprend chaque adresse IP disponible sur Internet, de 0.0.0.0 à 255.255.255.255. Même si votre déploiement compte une seule instance de fournisseur d'identité, vous pouvez modifier la plage d'adresses IP et ajouter d'autres plages afin d'exclure ou d'inclure des adresses IP spécifiques à la plage réseau par défaut. Vous pouvez créer d'autres plages réseau avec des adresses IP spécifiques que vous pouvez appliquer à des fins particulières.

Remarque La plage réseau par défaut (TOUTES LES PLAGES) et sa description (« un réseau pour toutes les plages ») sont modifiables. Pour modifier le nom et la description ou pour changer la langue du texte, accédez à la page Plages réseau et cliquez sur le nom de la plage réseau.

Prérequis

- Vous avez configuré des locataires pour votre déploiement de vRealize Automation et défini un lien Active Directory approprié pour prendre en charge l'authentification de base de l'identifiant et du mot de passe utilisateur Active Directory.
- Active Directory est installé et configuré pour être utilisé sur votre réseau.
- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

- 1 Sélectionnez **Administration > Directories Management > Plages réseau**.
- 2 Modifiez une plage réseau existante ou ajoutez une plage.

Option	Description
Modifier une plage réseau existante	Cliquez sur le nom de la plage réseau pour la modifier.
Ajouter une plage	Cliquez sur Ajouter une plage réseau pour ajouter une nouvelle plage.

- 3 Renseignez le formulaire.

Élément de formulaire	Description
Nom	Entrez un nom pour la plage réseau.
Description	Entrez une description pour la plage réseau.
Espaces View	L'option Espaces View s'affiche uniquement lorsque le module View est activé. Hôte de l'URL d'accès au client. Entrez l'URL d'accès à Horizon Client correspondant à la plage réseau. Port d'accès à Client. Entrez le numéro de port d'accès à Horizon Client correspondant à la plage réseau.
Plages d'adresses IP	Modifiez ou ajoutez des plages d'adresses IP jusqu'à ce que toutes les adresses IP souhaitées soient incluses et toutes les adresses IP non souhaitées soient exclues.

Suivant

- Associez chaque plage réseau à une instance de fournisseur d'identité.

- Associez les plages réseau à une règle de stratégie d'accès, si nécessaire. Reportez-vous à [Configuration de paramètres de stratégie d'accès](#).

Sélection des attributs à synchroniser avec l'annuaire

Lorsque vous configurez l'annuaire Directories Management à synchroniser avec Active Directory, vous devez spécifier les attributs utilisateur qui sont synchronisés avec l'annuaire. Avant de configurer l'annuaire, vous pouvez spécifier sur la page Attributs utilisateur, les attributs requis par défaut et, si vous le souhaitez, des attributs supplémentaires à mapper aux attributs Active Directory.

Lorsque vous configurez la page Attributs utilisateur avant la création de l'annuaire, vous pouvez faire passer les attributs par défaut de l'état obligatoire à l'état facultatif, marquer les attributs si nécessaire et ajouter des attributs personnalisés.

Pour obtenir la liste des attributs mappés par défaut, reportez-vous à [Gestion des attributs utilisateur synchronisés à partir d'Active Directory](#).

Une fois l'annuaire créé, vous pouvez faire passer un attribut obligatoire à l'état facultatif, et vous pouvez supprimer des attributs personnalisés. Il n'est pas possible de modifier un attribut pour le faire passer à l'état obligatoire.

Lorsque vous ajoutez d'autres attributs à synchroniser avec l'annuaire, une fois l'annuaire créé, accédez à la page Attributs mappés de l'annuaire pour mapper ces attributs à ceux d'Active Directory.

Procédure

- 1 Connectez-vous à vRealize Automation en tant qu'administrateur système ou administrateur de locataires.
- 2 Cliquez sur l'onglet Administration.
- 3 Sélectionnez **Directories Management > Attributs utilisateur**.
- 4 Dans la section Attributs par défaut, examinez la liste d'attributs obligatoires et apportez les modifications souhaitées pour refléter les attributs obligatoires.
- 5 Dans la section Attributs, ajoutez le nom d'attribut de l'annuaire Directories Management à la liste.
- 6 Cliquez sur **Enregistrer**.
L'état d'attribut par défaut est mis à jour et les attributs que vous avez ajoutés sont ajoutés à la liste d'attributs mappés de l'annuaire.
- 7 Une fois l'annuaire créé, accédez à la page Magasins d'identités et sélectionnez l'annuaire.
- 8 Cliquez sur **Paramètres de synchronisation > Attributs mappés**.
- 9 Dans le menu déroulant des attributs que vous avez ajoutés, sélectionnez l'attribut Active Directory à mapper.
- 10 Cliquez sur **Enregistrer**.

L'annuaire est mis à jour lors de sa prochaine synchronisation avec Active Directory.

Application de la stratégie d'accès par défaut

Le service Directories Management inclut une stratégie d'accès par défaut qui contrôle l'accès des utilisateurs à leurs portails d'applications. Il est possible de modifier la stratégie pour changer ses règles si nécessaire.

Lorsque vous activez des méthodes d'authentification autres qu'une authentification par mot de passe, vous devez modifier la stratégie par défaut pour ajouter la méthode d'authentification activée aux règles de la stratégie.

Chaque règle de la stratégie d'accès par défaut exige qu'un ensemble de critères soit satisfait pour accorder à l'utilisateur l'accès au portail des applications. Vous pouvez appliquer une plage réseau, déterminer le type d'utilisateur autorisé à accéder au contenu et sélectionner la méthode d'authentification souhaitée. Reportez-vous à [Gestion des stratégies d'accès](#).

Le nombre de tentatives effectuées par le service pour connecter un utilisateur à l'aide d'une méthode d'authentification donnée varie. Le service n'effectue qu'une seule tentative d'authentification pour Kerberos ou l'authentification par certificat. Si la tentative de connexion d'un utilisateur échoue, une tentative est effectuée sur la méthode d'authentification suivante de la règle. Le nombre maximal d'échecs de la tentative de connexion pour l'authentification par mot de passe Active Directory et RSA SecurID est de cinq par défaut. Lorsqu'un utilisateur enregistre cinq tentatives de connexion infructueuses, le service tente de connecter l'utilisateur en utilisant la méthode d'authentification suivante dans la liste. Lorsque toutes les méthodes d'authentification ont été utilisées sans succès, le service affiche un message d'erreur.

Application de méthodes d'authentification aux règles de stratégie

Seule la méthode d'authentification par mot de passe est configurée dans les règles de stratégie par défaut. Vous devez modifier les règles de stratégie pour sélectionner les autres méthodes d'authentification que vous avez configurées et définir l'ordre dans lequel les méthodes d'authentification sont utilisées pour l'authentification.

Prérequis

Activez et configurez les méthodes d'authentification que votre organisation prend en charge. Reportez-vous à [Intégration d'autres produits d'authentification de l'utilisateur à Directories Management](#)

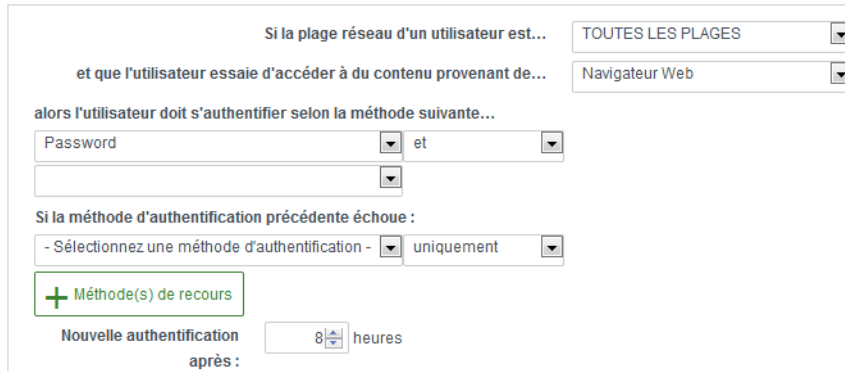
Procédure

- 1 Sélectionnez **Administration > Gestion des annuaires > Stratégies**
- 2 Cliquez sur la stratégie d'accès par défaut à modifier.
- 3 Pour modifier une règle de stratégie, cliquez sur la méthode d'authentification à modifier dans la colonne Règles de stratégie, méthode d'authentification.

Pour ajouter une nouvelle règle de stratégie, cliquez sur l'icône +.

- 4 Cliquez sur **Enregistrer** et de nouveau sur **Enregistrer** sur la page Stratégie.

Modifier une règle de stratégie



- 5 Cliquez sur **Enregistrer** et de nouveau sur **Enregistrer** sur la page Stratégie.

Configuration de Kerberos pour Directories Management

L'authentification Kerberos permet aux utilisateurs correctement connectés à leur domaine Active Directory d'accéder à leur portail d'applications sans devoir saisir de nouveau leurs informations d'identification. Vous devez activer l'authentification Windows pour permettre au protocole Kerberos de sécuriser les interactions entre les navigateurs des utilisateurs et le service Directories Management. Il n'est pas nécessaire de configurer directement Active Directory pour faire fonctionner Kerberos avec votre déploiement.

Actuellement, les interactions entre le navigateur d'un utilisateur et le service sont authentifiées par Kerberos sur les systèmes d'exploitation Windows seulement. L'accès au service à partir d'autres systèmes d'exploitation ne tire pas parti de l'authentification Kerberos.

■ Configuration de l'authentification Kerberos

Pour configurer le service Directories Management afin qu'il effectue l'authentification Kerberos, vous devez rejoindre le domaine et autoriser l'authentification Kerberos sur le connecteur Directories Management.

■ Configuration d'Internet Explorer pour accéder à l'interface Web

Vous devez configurer le navigateur Internet Explorer si Kerberos est configuré pour votre déploiement et si vous voulez accorder aux utilisateurs l'accès à l'interface Web à l'aide d'Internet Explorer.

■ Configuration de Firefox pour accéder à l'interface Web

Vous devez configurer le navigateur Firefox si Kerberos est configuré pour votre déploiement et si vous voulez accorder aux utilisateurs l'accès à l'interface Web via Firefox.

■ Configuration du navigateur Chrome pour accéder à l'interface Web

Vous devez configurer le navigateur Chrome si Kerberos est configuré pour votre déploiement et si vous voulez accorder aux utilisateurs l'accès à l'interface Web via Chrome.

Configuration de l'authentification Kerberos

Pour configurer le service Directories Management afin qu'il effectue l'authentification Kerberos, vous devez rejoindre le domaine et autoriser l'authentification Kerberos sur le connecteur Directories Management.

Procédure

- 1 En tant qu'administrateur de locataire, accédez à **Administration > Directories Management > Connecteurs**.
- 2 Sur la page Connecteurs du connecteur configuré pour l'authentification Kerberos, cliquez sur **Joindre le domaine**.
- 3 Sur la page Joindre le domaine, entrez les informations pour le domaine Active Directory.

Option	Description
Contrôleur	Saisissez le nom de domaine complet d'Active Directory. Le nom de domaine que vous entrez doit être le même domaine Windows que celui du serveur du connecteur.
Utilisateur du domaine	Saisissez le nom d'utilisateur d'un compte de l'instance d'Active Directory disposant des autorisations nécessaires pour joindre des systèmes à ce domaine Active Directory.
Mot de passe du domaine	Saisissez le mot de passe associé au Nom d'utilisateur AD. Ce mot de passe n'est pas stocké par Directories Management.

Cliquez sur **Enregistrer**.

La page Joindre le domaine est actualisée et affiche un message confirmant que vous êtes actuellement joint au domaine.

- 4 Dans la colonne Travailleur correspondant au connecteur, cliquez sur **Adaptateurs d'authentification**.
- 5 Cliquez sur **KerberosIldapAdapter**.
Vous serez redirigé vers la page de connexion du gestionnaire d'identité.
- 6 Cliquez sur **Modifier** sur la ligne KerberosIldapAdapter et configurez la page d'authentification de Kerberos.

Option	Description
Nom	Un nom est requis. Le nom par défaut est KerberosIldapAdapter. Vous pouvez modifier ce paramètre.
Attribut UID du répertoire	Entrez l'attribut de compte qui contient le nom d'utilisateur.
Activer l'authentification Windows	Sélectionnez cette option pour étendre les interactions d'authentification entre les navigateurs des utilisateurs et Directories Management.

Option	Description
Activer NTLM	Sélectionnez cette option pour activer l'authentification par protocole du gestionnaire de LAN NT (NTLM) uniquement si votre infrastructure Active Directory dépend de l'authentification NTLM.
Activer la redirection	Sélectionnez cette option si le DNS tourniquet et les équilibres de charge ne prennent pas en charge Kerberos. Les demandes d'authentification sont redirigées vers Rediriger le nom d'hôte. Si cette option est cochée, entrez le nom d'hôte de redirection dans la zone de texte Rediriger le nom d'hôte . Il s'agit généralement du nom d'hôte du service.

7 Cliquez sur **Enregistrer**.

Suivant

Ajoutez la méthode d'authentification à la stratégie d'accès par défaut. Accédez à **Administration > Directories Management > Stratégies**. Pour modifier les règles de stratégie par défaut et y ajouter la méthode d'authentification Kerberos dans le bon ordre d'authentification, cliquez ensuite sur **Modifier la stratégie par défaut**.

Configuration d'Internet Explorer pour accéder à l'interface Web

Vous devez configurer le navigateur Internet Explorer si Kerberos est configuré pour votre déploiement et si vous voulez accorder aux utilisateurs l'accès à l'interface Web à l'aide d'Internet Explorer.

L'authentification Kerberos fonctionne conjointement avec Directories Management sur les systèmes d'exploitation Windows.

Remarque N'effectuez pas ces étapes relatives à Kerberos sur d'autres systèmes d'exploitation.

Prérequis

Configurez le navigateur Internet Explorer pour chaque utilisateur ou fournissez les instructions aux utilisateurs, après avoir configuré Kerberos.

Procédure

- 1 Vérifiez que vous êtes connecté à Windows en tant qu'utilisateur du domaine.
- 2 Dans Internet Explorer, activez la connexion automatique.
 - a Sélectionnez **Outils > Options Internet > Sécurité**.
 - b Cliquez sur **Personnaliser le niveau**.
 - c Sélectionnez **Connexion automatique uniquement dans la zone intranet**.
 - d Cliquez sur **OK**.
- 3 Vérifiez que cette instance du dispositif virtuel du connecteur fait partie de la zone intranet locale.
 - a Utilisez Internet Explorer pour accéder à l'URL de connexion de Directories Management à l'adresse `https://myconnectorhost.domain/authenticate/`.
 - b Localisez la zone dans le coin inférieur droit de la barre d'état de la fenêtre du navigateur.
Si la zone est Intranet local, la configuration d'Internet Explorer est terminée.

- 4 Si la zone n'est pas Intranet local, ajoutez l'URL de connexion de Directories Management à la zone intranet.
 - a Sélectionnez **Outils > Options Internet > Sécurité > Intranet local > Sites**.
 - b Sélectionnez **Détecter automatiquement le réseau Intranet**.
 Si cette option n'est pas sélectionnée, sa sélection peut être suffisante pour ajouter à la zone intranet.
 - c (Facultatif) Si vous avez sélectionné **Détecter automatiquement le réseau Intranet**, cliquez sur **OK** jusqu'à ce que toutes les boîtes de dialogue soient fermées.
 - d Dans la boîte de dialogue Intranet local, cliquez sur **Avancé**.
 Une deuxième boîte de dialogue nommée Intranet local s'affiche.
 - e Tapez l'URL de Directories Management dans la zone de texte **Ajouter ce site Web à la zone**.
https://myconnectorhost.domain/authenticate/
 - f Cliquez sur **Ajouter > Fermer > OK**.
- 5 Vérifiez qu'Internet Explorer est autorisé à passer l'authentification Windows pour accéder au site de confiance.
 - a Dans la boîte de dialogue Options Internet, cliquez sur l'onglet **Avancé**.
 - b Sélectionnez **Activer l'authentification Windows intégrée**.
 Cette option prend effet seulement après le redémarrage d'Internet Explorer.
 - c Cliquez sur **OK**.
- 6 Connectez-vous à l'interface Web pour vérifier l'adresse.
 Si l'authentification Kerberos est réussie, l'URL de test vous redirige vers l'interface Web.

Le protocole Kerberos sécurise toutes les interactions entre cette instance Internet Explorer et Directories Management. Les utilisateurs peuvent à présent utiliser un accès à authentification unique pour leur portail Mes applications.

Configuration de Firefox pour accéder à l'interface Web

Vous devez configurer le navigateur Firefox si Kerberos est configuré pour votre déploiement et si vous voulez accorder aux utilisateurs l'accès à l'interface Web via Firefox.

L'authentification Kerberos fonctionne conjointement avec Directories Management sur les systèmes d'exploitation Windows.

Prérequis

Configurez le navigateur Firefox pour chaque utilisateur, ou communiquez des instructions aux utilisateurs après la configuration de Kerberos.

Procédure

- 1 Dans la zone de texte de l'URL du navigateur Firefox, saisissez `about:config` pour accéder aux paramètres avancés.
- 2 Cliquez sur **Je ferai attention, promis !**.
- 3 Double-cliquez sur **network.negotiate-auth.trusted-uris** dans la colonne Nom de l'option.
- 4 Tapez l'URL de Directories Management dans la zone de texte.
https://myconnectorhost.domain.com
- 5 Cliquez sur **OK**.
- 6 Double-cliquez sur **network.negotiate-auth.delegation-uris** dans la colonne Nom de l'option.
- 7 Tapez l'URL de Directories Management dans la zone de texte.
https://myconnectorhost.domain.com/authenticate/
- 8 Cliquez sur **OK**.
- 9 Testez la fonctionnalité de Kerberos en utilisant Firefox pour accéder à l'URL de connexion de . Par exemple, *https://myconnectorhost.domain.com/authenticate/*.

Si l'authentification Kerberos réussit, l'URL de test vous redirige vers l'interface Web.

Le protocole Kerberos sécurise toutes les interactions entre cette instance Firefox et Directories Management. Les utilisateurs peuvent utiliser un accès à authentification unique pour leur portail Mes applications.

Configuration du navigateur Chrome pour accéder à l'interface Web

Vous devez configurer le navigateur Chrome si Kerberos est configuré pour votre déploiement et si vous voulez accorder aux utilisateurs l'accès à l'interface Web via Chrome.

L'authentification Kerberos fonctionne conjointement avec Directories Management sur les systèmes d'exploitation Windows.

Remarque N'effectuez pas ces étapes relatives à Kerberos sur d'autres systèmes d'exploitation.

Prérequis

- Configurez Kerberos.
- Dans la mesure où Chrome utilise la configuration d'Internet Explorer pour activer l'authentification Kerberos, vous devez configurer Internet Explorer afin de permettre à Chrome d'utiliser la configuration d'Internet Explorer. Pour en savoir plus sur la procédure de configuration de Chrome pour l'authentification Kerberos, reportez-vous à la documentation de Google.

Procédure

- 1 Testez les fonctionnalités de Kerberos à l'aide du navigateur Chrome.

2 Connectez-vous à Directories Management sur <https://myconnectorhost.domain.com/authenticate/>.

Si l'authentification Kerberos réussit, l'URL de test vous redirige vers l'interface Web.

Si toutes les configuration relatives à Kerberos sont correctes, le protocole correspondant (Kerberos) sécurise toutes les interactions entre cette instance Chrome et Directories Management. Les utilisateurs peuvent utiliser un accès à authentification unique pour leur portail Mes applications.

Mise à niveau de connecteurs externes de gestion des répertoires

Si vous utilisez un connecteur externe avec votre configuration de gestion des répertoires vRealize Automation, il peut être nécessaire de le mettre à niveau de temps à autre.

Il peut être nécessaire de mettre à niveau un connecteur externe lors de la mise à niveau de la version de votre déploiement vRealize Automation ou si le build du nouveau connecteur fournit une fonction souhaitée.

Cette documentation s'applique uniquement aux utilisateurs qui ont déployé des dispositifs de connecteur supplémentaire autonome. Dans vRealize Automation, des dispositifs de connecteur externe sont utilisés, par exemple, avec l'authentification par carte à puce.

Par défaut, le connecteur utilise le site Web VMware pour la procédure de mise à niveau, qui requiert que le dispositif du connecteur soit connecté à Internet. Vous devez également configurer les paramètres du serveur proxy pour le dispositif du connecteur, si applicable.

Si votre instance du connecteur n'est pas connectée à Internet, vous pouvez effectuer la mise à niveau hors ligne. Pour une mise à niveau hors ligne, téléchargez le module de mise à niveau et configurez un serveur Web local pour qu'il héberge le fichier de mise à niveau.

Public visé

Ces informations sont destinées à toute personne qui installe, met à niveau et configure la gestion des répertoires. Les informations sont rédigées à l'intention d'administrateurs système Windows ou Linux expérimentés déjà familiarisés avec la technologie des machines virtuelles.

Préparation de la mise à niveau d'un connecteur externe

Pour préparer la mise à niveau d'un connecteur, vous devez rechercher les mises à niveau disponibles et configurer les paramètres du serveur proxy, le cas échéant.

- [Vérifier la disponibilité d'une mise à niveau de connecteur externe en ligne](#)

Si votre dispositif du connecteur est connecté à Internet, vous pouvez vérifier la disponibilité des mises à niveau en ligne à partir du dispositif.

- [Configurer les paramètres du serveur proxy pour le dispositif de connecteur externe](#)

Le dispositif du connecteur accède aux serveurs de mise à jour VMware par Internet. Si votre configuration réseau fournit un accès à Internet via un proxy HTTP, vous devez régler les paramètres de proxy pour le dispositif.

Vérifier la disponibilité d'une mise à niveau de connecteur externe en ligne

Si votre dispositif du connecteur est connecté à Internet, vous pouvez vérifier la disponibilité des mises à niveau en ligne à partir du dispositif.

Procédure

- 1 Connectez-vous au dispositif du connecteur en tant qu'utilisateur root.
- 2 Exécutez la commande suivante.

```
/usr/local/horizon/update/updatemgr.hzn updateinstaller
```

- 3 Exécutez la commande suivante pour rechercher une mise à niveau en ligne.

```
/usr/local/horizon/update/updatemgr.hzn check
```

Configurer les paramètres du serveur proxy pour le dispositif de connecteur externe

Le dispositif du connecteur accède aux serveurs de mise à jour VMware par Internet. Si votre configuration réseau fournit un accès à Internet via un proxy HTTP, vous devez régler les paramètres de proxy pour le dispositif.

Autorisez uniquement la gestion du trafic Internet sur votre serveur proxy. Pour vous assurer que le serveur proxy est correctement configuré, définissez le paramètre du trafic interne sur no-proxy dans le domaine.

Remarque Les serveurs proxy qui requièrent l'authentification ne sont pas pris en charge.

Prérequis

- Vérifiez que vous disposez du mot de passe racine pour le dispositif du connecteur.
- Vérifiez que vous disposez des informations du serveur proxy.

Procédure

- 1 Connectez-vous au dispositif du connecteur en tant qu'utilisateur racine.
- 2 Entrez YaST sur la ligne de commande pour exécuter l'utilitaire YaST.
- 3 Sélectionnez **Services réseau** dans le volet de gauche, puis sélectionnez **Proxy**.
- 4 Entrez les URL du serveur proxy dans les champs **URL de proxy HTTP** et **URL de proxy HTTPS**.
- 5 Sélectionnez **Terminer** et quittez l'utilitaire YaST.
- 6 Redémarrez le serveur Tomcat sur le dispositif virtuel du connecteur pour utiliser les nouveaux paramètres de proxy.

```
service horizon-workspace restart
```

Les serveurs de mise à jour VMware sont maintenant disponibles pour le dispositif du connecteur.

Mettre à niveau un connecteur externe en ligne

Vous pouvez mettre à niveau un connecteur externe de gestion des répertoires en ligne si vous disposez d'une connexion appropriée.

Prérequis

- Vérifiez que le dispositif du connecteur peut résoudre et atteindre l'adresse `vapp-updates.vmware.com` sur le port 80 via HTTP.
- Confirmez qu'une mise à niveau de connecteur existe. Exécutez la commande appropriée pour rechercher des mises à niveau. Reportez-vous à la rubrique *Vérifier la disponibilité d'une mise à niveau de connecteur Directories Management en ligne*.
- Vérifiez qu'au moins 2 Go d'espace disque sont disponibles sur la partition racine principale du dispositif.
- Vérifiez que le connecteur est correctement configuré.
- Prenez un snapshot de votre dispositif du connecteur pour le sauvegarder. Pour plus d'informations sur la création de snapshots, consultez la documentation de vSphere.
- Si un serveur proxy HTTP est requis pour l'accès HTTP sortant, configurez les paramètres du serveur proxy pour le dispositif du connecteur. Reportez-vous à la rubrique *Configurer les paramètres du serveur proxy pour le dispositif de connecteur Directories Management*.

Procédure

- 1 Connectez-vous au dispositif du connecteur en tant qu'utilisateur root.
- 2 Exécutez la commande suivante.

```
/usr/local/horizon/update/updatemgr.hzn updateinstaller
```

- 3 Exécutez la commande suivante pour vérifier qu'une mise à niveau en ligne existe.

```
/usr/local/horizon/update/updatemgr.hzn check
```

- 4 Exécutez la commande suivante pour mettre à jour le dispositif.

```
/usr/local/horizon/update/updatemgr.hzn update
```

Les messages générés pendant la mise à niveau sont enregistrés dans le fichier `update.log` à l'emplacement `/opt/vmware/var/log/update.log`.

- 5 Exécutez de nouveau la commande `updatemgr.hzn check` pour vérifier qu'une mise à jour plus récente n'existe pas.

```
/usr/local/horizon/update/updatemgr.hzn check
```

6 Vérifiez la version du dispositif mis à niveau.

```
vamcli version --appliance
```

La nouvelle version est affichée.

7 Redémarrez le dispositif du connecteur.

```
reboot
```

Mettre à niveau un connecteur externe hors ligne

Si votre dispositif de connecteur de gestion des répertoires vRealize Automation ne peut pas se connecter à Internet pour la mise à niveau, vous pouvez effectuer une mise à niveau hors ligne. Vous devez installer un référentiel de mise à niveau sur un serveur Web local et configurer le dispositif du connecteur afin qu'il utilise le serveur Web local pour la mise à niveau.

Prérequis

- Vérifiez qu'une mise à niveau de connecteur existe. Rendez-vous sur le site Téléchargements My VMware à l'adresse my.vmware.com pour voir s'il existe des mises à niveau.
- Vérifiez qu'au moins 2 Go d'espace disque sont disponibles sur la partition racine principale du dispositif.
- Vérifiez que le connecteur est correctement configuré.
- Prenez un snapshot de votre dispositif de connecteur pour le sauvegarder. Pour plus d'informations sur la création de snapshots, consultez la documentation de vSphere.
- Configurez le dispositif du connecteur afin qu'il utilise un serveur Web local pour héberger le fichier de mise à niveau. Reportez-vous à la section Préparer un serveur Web local pour une mise à niveau hors ligne.

Procédure

1 Préparer un serveur Web local pour une mise à niveau hors ligne

Avant de démarrer la mise à niveau hors ligne du connecteur, préparez le serveur Web local en créant une structure de répertoire incluant un sous-répertoire pour le dispositif du connecteur.

2 Configurer le connecteur et effectuer une mise à niveau hors ligne

Configurez le dispositif du connecteur pour qu'il pointe vers le serveur Web local afin d'effectuer une mise à niveau hors ligne. Mettez ensuite le dispositif à niveau.

Préparer un serveur Web local pour une mise à niveau hors ligne

Avant de démarrer la mise à niveau hors ligne du connecteur, préparez le serveur Web local en créant une structure de répertoire incluant un sous-répertoire pour le dispositif du connecteur.

Prérequis

- Téléchargez le fichier `identity-manager-connector-versionNumber-buildNumber-updaterepo.zip` sur My VMware. Allez sur le site my.vmware.com, accédez à la page Téléchargement VMware Identity Manager et téléchargez le fichier répertorié sous **Package de mise à niveau hors ligne VMware Identity Manager Connector**.
- Si vous utilisez un serveur Web IIS, configurez le serveur Web pour qu'il autorise les caractères spéciaux dans les noms de fichier. Vous configurez cela dans la section **Filtrage des demandes** en sélectionnant l'option **Autoriser le double-échappement**.

Procédure

- 1 Créez un répertoire sur le serveur Web à l'adresse `http://YourWebServer/VM/` et copiez le fichier zip téléchargé dessus.
- 2 Vérifiez que votre serveur Web inclut des types mime pour `.sig` (texte/brut) et `.sha256` (texte/brut). Sans ces types mime, votre serveur Web ne parvient pas à rechercher les mises à jour.
- 3 Décompressez le fichier.
Le contenu du fichier ZIP extrait est servi par `http://YourWebServer/VM/`.
Le fichier extrait contient les sous-répertoires suivants : `/manifest` et `/package-pool`.
- 4 Exécutez la commande `updateLocal.hzn` suivante pour vérifier que l'URL dispose d'un contenu de mise à jour valide.

```
/usr/local/horizon/update/updatelocal.hzn checkurl http://YourWebServer/VM
```

Configurer le connecteur et effectuer une mise à niveau hors ligne

Configurez le dispositif du connecteur pour qu'il pointe vers le serveur Web local afin d'effectuer une mise à niveau hors ligne. Mettez ensuite le dispositif à niveau.

Prérequis

Préparer un serveur Web local pour une mise à niveau hors ligne.

Procédure

- 1 Connectez-vous au dispositif du connecteur en tant qu'utilisateur racine.

- 2 Exécutez la commande suivante pour configurer un référentiel de mise à niveau qui utilise un serveur Web local.

```
/usr/local/horizon/update/updatelocal.hzn seturl http://Votre_serveur_Web/VM/
```

Remarque Pour annuler la configuration et pouvoir de nouveau effectuer une mise à niveau en ligne, vous pouvez exécuter la commande suivante.

```
/usr/local/horizon/update/updatelocal.hzn setdefault
```

- 3 Effectuez la mise à niveau.

- a Exécutez la commande suivante.

```
/usr/local/horizon/update/updatemgr.hzn updateinstall
```

- b Exécutez la commande suivante pour vérifier la version de la mise à niveau disponible.

```
/usr/local/horizon/update/updatemgr.hzn check
```

- c Exécutez la commande suivante pour mettre à jour le connecteur.

```
/usr/local/horizon/update/updatemgr.hzn update
```

Les messages générés pendant la mise à niveau sont enregistrés dans le fichier `update.log` à l'emplacement `/opt/vmware/var/log/update.log`.

- d Exécutez de nouveau la commande `updatemgr.hzn check`.

```
/usr/local/horizon/update/updatemgr.hzn check
```

- e Vérifiez la version du dispositif mis à niveau.

```
vamcli version --appliance
```

La commande doit afficher la nouvelle version.

- f Redémarrez le dispositif du connecteur.

Par exemple, à partir de la ligne de commande, exécutez la commande suivante.

```
reboot
```

La mise à niveau du connecteur est terminée.

Configurer des paramètres après la mise à niveau d'un connecteur externe

Après la mise à niveau vers le connecteur 2016.3.1.0 ou une version plus récente, il peut être nécessaire de configurer certains paramètres.

Rejoindre un domaine avec l'authentification Kerberos

Si vous utilisez l'authentification Kerberos ou des annuaires Active Directory (authentification Windows intégrée), vous devez quitter le domaine et le rejoindre. Cela est obligatoire pour tous les dispositifs virtuels de connecteur dans votre déploiement.

- 1 Sélectionnez **Administration > Gestion des annuaires > Connecteurs**.
- 2 Sur la page Connecteurs, pour chaque connecteur utilisé pour l'authentification Kerberos ou un répertoire Active Directory (authentification Windows intégrée), cliquez sur **Quitter le domaine**.
- 3 Pour joindre le domaine, vous avez besoin d'informations d'identification Active Directory avec les privilèges pour joindre le domaine. Consultez [Joindre une machine de connecteur à un domaine](#) pour plus d'informations.
- 4 Si vous utilisez l'authentification Kerberos, activez de nouveau l'adaptateur d'authentification Kerberos. Pour accéder à la page Adaptateurs d'authentification, sur la page Connecteurs, cliquez sur le lien approprié dans la colonne **Employé** et sélectionnez l'onglet **Adaptateurs d'authentification**.
- 5 Vérifiez que les autres adaptateurs d'authentification que vous utilisez sont activés.

Mettre à jour la page Domaines

Si vous utilisez Active Directory (authentification Windows intégrée), ou Active Directory sur LDAP avec l'option **Cet annuaire prend en charge l'emplacement du service DNS** activée, enregistrez la page Domaines de l'annuaire.

- 1 Sélectionnez **Administration > Gestion des annuaires > Annuaires**.
- 2 Sélectionnez l'annuaire voulu pour le modifier.
- 3 Fournissez le mot de passe pour l'utilisateur ND Bind et cliquez sur **Enregistrer**.
- 4 Cliquez sur **Paramètres de synchronisation** sur la gauche de la page et sélectionnez l'onglet **Domaines**.
- 5 Cliquez sur **Enregistrer**.

Emplacement du service DNS et contrôleurs de domaine

Remarque Dans le connecteur 2016.3.1.0 et versions ultérieures, un fichier `domain_krb.properties` est créé et rempli automatiquement avec des contrôleurs de domaine lorsqu'un annuaire avec l'option **Emplacement du service DNS** activée est créé. Lorsque vous enregistrez la page Domaines après la mise à niveau, si vous disposiez d'un fichier `domain_krb.properties` dans votre déploiement d'origine, le fichier est mis à jour avec les domaines que vous avez pu ajouter par la suite et qui n'étaient pas dans le fichier. Si vous ne disposiez pas d'un fichier `domain_krb.properties` dans votre déploiement d'origine, le fichier est créé et rempli automatiquement avec des contrôleurs de domaine. Reportez-vous à la section [À propos de la sélection des contrôleurs de domaine](#) pour plus d'informations sur le fichier `domain_krb.properties`.

Dépannage des erreurs de mise à niveau de connecteur externe

Vous pouvez dépanner les problèmes de mise à niveau de connecteur externe de gestion des répertoires vRA en examinant les journaux d'erreur. Si le connecteur ne démarre pas, vous pouvez rétablir une instance précédente en restaurant un snapshot.

■ Examen des journaux d'erreur de mise à niveau

Résolvez les erreurs qui se produisent lors d'une mise à niveau en examinant les journaux d'erreur. Les fichiers journaux de mise à niveau se trouvent dans le répertoire `/opt/vmware/var/log`.

■ Restauration de snapshots du connecteur

Si le connecteur ne démarre pas correctement après une mise à niveau et que vous ne pouvez pas résoudre le problème en examinant les journaux d'erreur de mise à niveau et en exécutant à nouveau la commande de mise à niveau, vous pouvez restaurer une instance précédente du connecteur.

■ Collecter un bundle de fichiers journaux

Vous pouvez collecter un bundle de fichiers journaux à envoyer au support VMware. Vous obtenez le bundle sur la page de configuration du connecteur.

Examen des journaux d'erreur de mise à niveau

Résolvez les erreurs qui se produisent lors d'une mise à niveau en examinant les journaux d'erreur. Les fichiers journaux de mise à niveau se trouvent dans le répertoire `/opt/vmware/var/log`.

Si des erreurs se sont produites, le connecteur peut ne pas démarrer après la mise à niveau.

Procédure

- 1 Connectez-vous au dispositif du connecteur.
- 2 Accédez au répertoire `/opt/vmware/var/log`.
- 3 Ouvrez le fichier `update.log` et consultez les messages d'erreur.
- 4 Résolvez les erreurs et exécutez de nouveau la commande de mise à niveau. La commande de mise à niveau reprend au point où elle s'est arrêtée.

Remarque Vous pouvez également restaurer un snapshot et réexécuter la mise à jour.

Restauration de snapshots du connecteur

Si le connecteur ne démarre pas correctement après une mise à niveau et que vous ne pouvez pas résoudre le problème en examinant les journaux d'erreur de mise à niveau et en exécutant à nouveau la commande de mise à niveau, vous pouvez restaurer une instance précédente du connecteur.

Procédure

- ◆ Restaurez l'un des snapshots que vous avez pris comme sauvegarde de votre instance du connecteur d'origine. Pour plus d'informations, consultez la documentation de vSphere.

Collecter un bundle de fichiers journaux

Vous pouvez collecter un bundle de fichiers journaux à envoyer au support VMware. Vous obtenez le bundle sur la page de configuration du connecteur.

Les fichiers journaux suivants sont collectés dans le bundle.

Tableau 2-9. Fichiers journaux

Composant	Emplacement du fichier journal	Description
Journaux Apache Tomcat (catalina.log)	/opt/vmware/horizon/workspace/logs/catalina.log	Apache Tomcat enregistre les messages qui ne sont pas enregistrés dans d'autres fichiers journaux.
Journaux du Programme de configuration (configurator.log)	/opt/vmware/horizon/workspace/logs/configurator.log	Requêtes que Configurator reçoit du client REST et de l'interface Web.
Journaux Connector (connector.log)	/opt/vmware/horizon/workspace/logs/connector.log	Enregistrement de chaque demande reçue de l'interface Web. Chaque entrée de journal inclut également l'URL, l'horodatage et les exceptions de la requête. Aucune action de synchronisation n'est enregistrée.

Procédure

- 1 Connectez-vous à la page de configuration du connecteur à l'adresse <https://connectorURL:8443/cfg/logs>.
- 2 Cliquez sur **Préparer le bundle de journaux**.
- 3 Téléchargez le bundle et envoyez-le au support VMware.

Scénario : configurer un lien Active Directory pour une instance hautement disponible de vRealize Automation

En tant qu'administrateur de locataire, vous souhaitez configurer un annuaire Active Directory sur une connexion d'annuaire LDAP pour prendre en charge l'authentification des utilisateurs pour votre développement vRealize Automation hautement disponible.

Chaque instance du dispositif vRealize Automation inclut un connecteur qui prend en charge l'authentification de l'utilisateur, bien qu'un seul connecteur soit habituellement configuré pour exécuter la synchronisation d'annuaire. Le choix du connecteur devant faire office de connecteur de synchronisation est sans incidence. Afin de prendre en charge la haute disponibilité pour la fonctionnalité Gestion des annuaires, configurez un second connecteur qui correspond au second dispositif vRealize Automation. Ce connecteur doit se connecter au fournisseur d'identité et pointer vers la même instance d'Active Directory. Grâce à cette configuration, l'échec d'un dispositif est compensé par la reprise de la gestion de l'authentification de l'utilisateur par l'autre dispositif.

Dans un environnement de haute disponibilité, tous les nœuds doivent servir les mêmes instances d'Active Directory, les mêmes utilisateurs, méthodes d'authentification, etc. Pour ce faire, la méthode la plus directe consiste à promouvoir le fournisseur d'identité auprès du cluster, en définissant l'hôte de l'équilibrage de charge en tant qu'hôte du fournisseur d'identité. Grâce à cette configuration, toutes les demandes d'authentification sont dirigées vers l'équilibrage de charge, qui les transmet à son tour au connecteur approprié.

Prérequis

- Installez un déploiement vRealize Automation distribué avec des équilibres de charge appropriés. Reportez-vous à *Installation de vRealize Automation 7.3*.
- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

- 1 Sélectionnez **Administration > Gestion des répertoires > Répertoires**.
- 2 Cliquez sur **Ajouter un annuaire**.
- 3 Entrez vos paramètres de compte Active Directory spécifiques, puis acceptez les options par défaut.

Option	Exemple d'entrée
Nom de l'annuaire	Ajoutez l'adresse IP de votre nom de domaine Active Directory.
Connecteur de synchronisation	Chaque dispositif vRealize Automation contient un connecteur. Utilisez l'un des connecteurs disponibles.
Nom unique de base	Entrez le nom unique (DN) du point de départ des recherches sur le serveur d'annuaire. Par exemple, cn=users,dc=corp,dc=local .
Nom unique de liaison	Entrez le nom unique (DN) complet, incluant le nom commun (CN), d'un compte d'utilisateur Active Directory qui dispose de privilèges de recherche d'utilisateurs. Par exemple, cn=config_admin infra,cn=users,dc=corp,dc=local .
Mot de passe du nom unique de liaison	Entrez le mot de passe Active Directory du compte autorisé à rechercher des utilisateurs.

- 4 Cliquez sur **Tester la connexion** pour tester la connexion vers l'annuaire configuré.
Si la connexion échoue, vérifiez vos entrées pour tous les champs et consultez, si besoin, votre administrateur système.
- 5 Cliquez sur **Enregistrer et Suivant**.
La page Sélectionnez les domaines apparaît avec la liste des domaines.
- 6 Laissez le domaine par défaut sélectionné et cliquez sur **Suivant**.
- 7 Vérifiez que les noms d'attribut sont mappés sur les bons attributs d'Active Directory. Sinon, sélectionnez le bon attribut d'Active Directory dans le menu déroulant. Cliquez sur **Suivant**.

8 Sélectionnez les groupes et les utilisateurs que vous souhaitez synchroniser.

- a Cliquez sur l'icône **Ajouter** (+).
- b Entrez le domaine de l'utilisateur et cliquez sur **Rechercher des groupes**.
Par exemple, **cn=users,dc=corp,dc=local**.
- c Cochez la case **Tout sélectionner**.
- d Cliquez sur **Sélectionner**.
- e Cliquez sur **Suivant**.
- f Cliquez sur + pour ajouter des utilisateurs supplémentaires. Par exemple, effectuez la saisie sous la forme **CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com**.

Pour exclure des utilisateurs, cliquez sur + pour créer un filtre permettant d'exclure certains types d'utilisateurs. Vous pouvez sélectionner un attribut d'utilisateur à filtrer, la règle de requête et sa valeur.
- g Cliquez sur **Suivant**.

9 Examiner la page pour voir combien d'utilisateurs et de groupes se synchronisent avec l'annuaire, puis cliquez sur **Synchroniser l'annuaire**.

Le processus de synchronisation d'annuaire prend un certain temps, mais s'exécute en arrière-plan et vous pouvez continuer à travailler.

10 Configurez un deuxième connecteur pour prendre en charge la haute disponibilité.

- a Connectez-vous à l'équilibrage de charge du déploiement vRealize Automation en tant qu'administrateur de locataire.

L'URL de l'équilibrage de charge est *load balancer address/vcac/org/tenant_name*.
- b Sélectionnez **Administration > Directories Management > Fournisseurs d'identité**.
- c Cliquez sur le fournisseur d'identité actuellement utilisé dans le système.

L'annuaire et le connecteur existants qui fournissent une gestion des identités de base s'affichent.
- d Cliquez sur la liste déroulante **Ajouter un connecteur**, puis sélectionnez le connecteur correspondant à votre dispositif vRealize Automation secondaire.
- e Dans la zone de texte **Mot de passe du DN de liaison** qui s'affiche à la sélection du connecteur, entrez le mot de passe correspondant.
- f Cliquez sur **Ajouter un connecteur**.
- g Modifiez le nom d'hôte pour pointer vers votre équilibrage de charge.

Vous avez connecté l'annuaire Active Directory de votre entreprise à vRealize Automation et configuré la gestion des annuaires pour la haute disponibilité.

Suivant

Pour fournir une sécurité renforcée, vous pouvez configurer la confiance bidirectionnelle entre votre fournisseur d'identité et votre annuaire Active Directory. Reportez-vous à [Configurer une relation de confiance bidirectionnelle entre vRealize Automation et Active Directory](#).

Configurez les connecteurs externes pour la carte à puce et l'authentification à des fournisseur d'identité tiers dans vRealize Automation

Un administrateur système doit configurer un connecteur externe pour votre déploiement vRealize Automation à l'aide de la gestion des annuaires si vous utilisez des fournisseurs d'identité tiers tels que l'authentification Kerberos ou par carte à puce.

La gestion des annuaires prend en charge plusieurs fournisseurs d'identité et clusters de connecteurs pour chaque annuaire Active Directory configuré. Pour utiliser un fournisseur d'identité tiers ou l'authentification par carte à puce, vous pouvez configurer un connecteur externe unique ou un cluster de connecteurs avec un fournisseur d'identité approprié derrière un équilibrage de charge qui permet le relais SSL. Consultez [Gestion des connecteurs et des clusters de connecteurs](#) pour plus d'informations.

Reportez-vous à la section [Mise à niveau de connecteurs externes de gestion des répertoires](#) pour plus d'informations sur la mise à jour d'un connecteur externe.

Diverses options de configuration de certificats sont disponibles à utiliser avec l'authentification par carte à puce. Reportez-vous à [Configuration d'un certificat ou d'un adaptateur de carte à puce pour Directories Management](#).

Prérequis

- Configurez une connexion Active Directory appropriée à utiliser avec votre déploiement vRealize Automation.
- Téléchargez le fichier OVA requis pour configurer un connecteur depuis [Outils et SDK de VMware vRealize Automation](#).
- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

1 Générer un jeton d'activation de connecteur

Avant de déployer le dispositif virtuel du connecteur à utiliser pour l'authentification par carte à puce, générez un code d'activation pour le nouveau connecteur à partir de la console vRealize Automation. Le code d'activation est utilisé pour établir une communication entre la gestion des annuaires et le connecteur.

2 Déployer le fichier OVA du connecteur

Après le téléchargement du fichier OVA, vous pouvez le déployer à l'aide de VMware vSphere Client ou de vSphere Web Client.

3 Configurer les réglages de Connector

Après le déploiement du fichier OVA du connecteur, vous devez exécuter l'assistant de configuration pour activer le dispositif et configurer les mots de passe d'administrateur.

4 Appliquer une autorité de certification publique

Lorsque la gestion des annuaires est installée, un certificat de serveur SSL par défaut est généré. Vous pouvez utiliser le certificat par défaut à des fins de test, mais vous devez générer et installer des certificats SSL commerciaux pour les environnements de production.

5 Créer un fournisseur d'identité d'espace de travail

Vous devez créer un fournisseur d'identité d'espace de travail à utiliser avec un connecteur externe.

6 Configurer l'authentification par certificat et configurer les règles de stratégie d'accès par défaut

Vous devez configurer votre connecteur externe à utiliser avec votre annuaire Active Directory et domaine de vRealize Automation.

Générer un jeton d'activation de connecteur

Avant de déployer le dispositif virtuel du connecteur à utiliser pour l'authentification par carte à puce, générez un code d'activation pour le nouveau connecteur à partir de la console vRealize Automation. Le code d'activation est utilisé pour établir une communication entre la gestion des annuaires et le connecteur.

Vous pouvez configurer un connecteur unique ou un cluster de connecteurs. Si vous souhaitez utiliser un cluster de connecteurs, répétez cette procédure pour chaque connecteur requis.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

- 1 Sélectionnez **Administration > Gestion des annuaires > Connecteurs**.
- 2 Tapez un nom pour le nouveau connecteur dans la zone de texte **Nom ID du connecteur**.
- 3 Appuyez sur **Entrer**.
Le code d'activation du connecteur s'affiche dans la zone **Code d'activation du connecteur**.
- 4 Copiez le code d'activation à utiliser dans la configuration du connecteur à l'aide du fichier OVA.

Déployer le fichier OVA du connecteur

Après le téléchargement du fichier OVA, vous pouvez le déployer à l'aide de VMware vSphere Client ou de vSphere Web Client.

Vous déployez le fichier OVA à l'aide de vSphere Client ou vSphere Web Client.

Prérequis

- Identifiez les enregistrements DNS et le nom d'hôte à utiliser pour le déploiement du fichier OVA d'connector.

- Avec vSphere Web Client, utilisez les navigateurs Firefox ou Chrome. N'utilisez pas Internet Explorer pour déployer le fichier OVA.
- Téléchargez le fichier OVA requis pour configurer un connecteur depuis [Outils et SDK de VMware vRealize Automation](#).

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, sélectionnez **Fichier > Déployer le modèle OVF**.
- 2 Dans les pages Déployer le modèle OVF, entrez les informations spécifiques de votre déploiement d'connector.

Page	Description
Source	Localisez l'emplacement du module OVA ou entrez une URL spécifique.
Détails du module OVA	Vérifiez que vous avez sélectionné la version correcte.
Licence	Lisez l'accord de licence d'utilisateur final et cliquez sur Accepter .
Nom et emplacement	Saisissez un nom pour le dispositif virtuel. Le nom doit être unique dans le dossier d'inventaire et contenir au maximum 80 caractères. Les noms sont sensibles à la casse. Sélectionnez un emplacement pour le dispositif virtuel.
Hôte / Cluster	Sélectionnez l'hôte ou le cluster pour exécuter le modèle déployé.
Pool de ressources	Sélectionnez le pool de ressources.
Stockage	Sélectionnez l'emplacement de stockage des fichiers des machines virtuelles.
Format du disque	Sélectionnez le format de disque pour les fichiers. Pour les environnements de production, sélectionnez le format Provisionnement statique . Utilisez le format Provisionnement dynamique pour les évaluations et les tests.
Mappage réseau	Mappez les réseaux de votre environnement vers les réseaux du modèle OVF.
Propriétés	<ol style="list-style-type: none"> a Dans le champ Paramètre de fuseau horaire, sélectionnez le fuseau horaire correspondant. b La case Programme d'amélioration du produit est cochée par défaut. VMware collecte des données anonymes sur votre déploiement afin d'améliorer la réponse de VMware aux exigences des utilisateurs. Décochez la case si vous ne voulez pas que les données soient collectées. c Dans le champ Nom de l'hôte, entrez le nom d'hôte à utiliser. Si ce champ est vide, le DNS inversé est utilisé pour rechercher le nom d'hôte. d Pour configurer l'adresse IP statique d'connector, entrez l'adresse de chacun des éléments suivants : Passerelle par défaut, DNS, Adresse IP et Masque réseau. <p>Important Si l'un des quatre champs d'adresse, y compris Nom d'hôte, est vide, le protocole DHCP est utilisé.</p> <p>Pour configurer le protocole DHCP, laissez les champs d'adresse vides.</p>
Prêt à terminer	Passez vos sélections en revue et cliquez sur Terminer .

Selon la vitesse de votre réseau, le déploiement peut nécessiter plusieurs minutes. Vous pouvez voir la progression dans la boîte de dialogue de progression.

- 3 Lorsque le déploiement est terminé, sélectionnez le dispositif , cliquez avec le bouton droit et sélectionnez **Alimentation > Mettre sous tension**.

Le dispositif est initialisé. Vous pouvez accéder à l'onglet **Console** pour voir les détails. Une fois l'initialisation du dispositif virtuel terminée, l'écran de la console affiche la version de et les URL pour vous connecter à l'Assistant de configuration de , afin de terminer la configuration.

Suivant

Utilisez l'Assistant de configuration pour ajouter le code d'activation et les mots de passe d'administration.

Configurer les réglages de Connector

Après le déploiement du fichier OVA du connecteur, vous devez exécuter l'assistant de configuration pour activer le dispositif et configurer les mots de passe d'administrateur.

Prérequis

- Vous avez généré un code d'activation pour le connecteur.
- Assurez-vous que le dispositif du connecteur est sous tension et que vous connaissez l'URL du connecteur.
- Collectez une liste des mots de passe à utiliser pour l'administrateur du connecteur, le compte racine et le compte sshuser.

Procédure

- 1 Pour exécuter l'assistant de configuration, entrez l'URL de connector qui s'est affichée dans l'onglet Console une fois l'OVA déployé.
- 2 Sur la page d'accueil, cliquez sur **Continuer**.
- 3 Créez des mots de passe forts pour les comptes d'administrateur de dispositif virtuel connector suivants.

Les mots de passe forts doivent contenir au moins huit caractères, des majuscules et des minuscules, et au moins un chiffre ou caractère spécial.

Option	Description
Administrateur du dispositif	<p>Créez le mot de passe de l'administrateur du dispositif. Le nom d'utilisateur est admin et ne peut pas être modifié. Vous utilisez ce compte et ce mot de passe pour vous connecter aux services connector afin de gérer les certificats, les mots de passe des dispositifs et la configuration syslog.</p> <hr/> <p>Important Le mot de passe de l'utilisateur Admin doit contenir au moins 6 caractères.</p>
Compte racine	Un mot de passe racine VMware par défaut a été utilisé pour installer le dispositif connector. Créez un mot de passe racine.
Compte sshuser	Créez le mot de passe à utiliser pour l'accès à distance au dispositif du connecteur.

- 4 Cliquez sur **Continuer**.

- 5 Sur la page Activer le connecteur, collez le code d'activation et cliquez sur **Continuer**.
- 6 Si vous utilisez un certificat autosigné sur le connecteur interne vRealize Automation, vous pouvez obtenir le certificat approprié en exécutant la commande suivante sur le dispositif
vRealize Automation : `cat /etc/apache2/server-cert.pem`

Sélectionnez l'onglet **Mettre fin à SSL sur un équilibrage de charge**, puis cliquez sur le lien pour `/horizon_workspace_rootca.pem`.

Le code d'activation est vérifié et une communication entre le service et l'instance du connecteur est établie pour terminer la configuration du connecteur.

Suivant

Dans le service, configurez votre environnement selon vos besoins. Par exemple, si vous avez ajouté un connecteur supplémentaire, car vous voulez synchroniser deux annuaires Authentification Windows intégrée, créez l'annuaire et associez-le au nouveau connecteur.

Appliquer une autorité de certification publique

Lorsque la gestion des annuaires est installée, un certificat de serveur SSL par défaut est généré. Vous pouvez utiliser le certificat par défaut à des fins de test, mais vous devez générer et installer des certificats SSL commerciaux pour les environnements de production.

Remarque Si le Directories Management pointe vers un équilibrage de charge, le certificat SSL est appliqué à celui-ci.

Vous devez vérifier la valeur **Marquer cette clé comme exportable** lors de l'importation d'un certificat.

Vous devez uniquement spécifier le nom commun ou le nom de domaine du site d'autorité de certification, si vous générez une demande de signature d'un certificat personnalisé.

Prérequis

Générez une demande de signature de certificat (CSR) pour obtenir un certificat valide et signé d'une autorité de certification. Si votre entreprise fournit des certificats SSL signés par une autorité de certification, vous pouvez les utiliser. Le certificat doit être au format PEM.

Procédure

- 1 Connectez-vous à la page administrative du dispositif du connecteur en tant qu'utilisateur Admin à l'emplacement suivant :
`https://myconnector.mycompany:8443/cfg`
- 2 Dans la console d'administration, cliquez sur **Paramètres du dispositif**.
La configuration VA est sélectionnée par défaut.
- 3 Cliquez sur **Gérer les Configurations**.
- 4 Entrez le mot de passe de l'utilisateur Admin du serveur VMware Identity Manager.
- 5 Sélectionnez **Installer le certificat**.

- 6 Dans l'onglet Interrompre SSL sur un dispositif Identity Manager, sélectionnez **Certificat personnalisé**.
- 7 Dans la zone de texte **Chaîne de certificat SSL**, collez les certificats hôte, intermédiaire et racine, dans cet ordre.

Le certificat SSL ne fonctionne que si vous incluez toute la chaîne de certificat dans le bon ordre. Pour chaque certificat, copiez tout ce qui se trouve entre les lignes -----BEGIN CERTIFICATE----- et -----END CERTIFICATE-----, en incluant celles-ci.

Vérifiez que le certificat inclut le nom d'hôte FQDN.
- 8 Collez la clé privée dans la zone de texte Clé privée. Copiez tout ce qui se trouve entre les lignes -----BEGIN RSA PRIVATE KEY et ---END RSA PRIVATE KEY.
- 9 Cliquez sur **Enregistrer**.

Exemple : Exemples de certificat

Exemple de chaîne de certificat
-----BEGIN CERTIFICATE-----
jIQt9WdR9Vpg3WQT5+C3HU17bUOwvhp/r0+
...
...
...
W53+O05j5xsxzDJfWr1lqBIFF/OkIYCPcyK1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
WdR9Vpg3WQT5+C3HU17bUOwvhp/rjIQt90+
...
...
...
O05j5xsxzDJfWr1lqBIFF/OkIYCPW53+cyK1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
dR9Vpg3WQTjIQt9W5+C3HU17bUOwvhp/r0+
...
...
...
5j5xsxzDJfWr1lqW53+O0BIFF/OkIYCPcyK1
-----END CERTIFICATE-----

Exemple de clé privée

-----BEGIN RSA PRIVATE KEY-----

jIQtvg3WQT5+C3HU17bU9WdR9VpOwvhp/r0+

...

...

...

1lqBIFFW53+O05j5xsxzDJfWr/OklYCPcyK1

-----END RSA PRIVATE KEY-----

Créer un fournisseur d'identité d'espace de travail

Vous devez créer un fournisseur d'identité d'espace de travail à utiliser avec un connecteur externe.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

- 1 Sélectionnez **Administration > Gestion des annuaires > Fournisseurs d'identité**.
- 2 Sélectionnez **Ajouter un fournisseur d'identité**.
- 3 Sélectionnez **Créer un espace de travail IDP** sur le menu affiché.
- 4 Entrez un nom pour le fournisseur d'identité dans le champ **Nom du fournisseur d'identité**.
- 5 Sélectionnez l'annuaire qui correspond aux utilisateurs qui utiliseront ce fournisseur d'identité.

L'annuaire sélectionné détermine quels connecteurs sont affichés pour sélection avec ce fournisseur d'identité.

- 6 Sélectionnez le ou les connecteurs externes que vous avez configurés pour l'authentification par carte à puce.

Remarque Si le déploiement se trouve derrière un équilibrage de charge, entrez l'URL de l'équilibrage de charge.

- 7 Sélectionnez le réseau pour accéder à ce fournisseur d'identité.
- 8 Cliquez sur **Ajouter**.

Configurer l'authentification par certificat et configurer les règles de stratégie d'accès par défaut

Vous devez configurer votre connecteur externe à utiliser avec votre annuaire Active Directory et domaine de vRealize Automation.

Prérequis

Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

- 1 Sélectionnez **Administration > Directories Management > Connecteurs**.
- 2 Sélectionnez le connecteur souhaité dans la colonne **Travailleur**.
Le travailleur sélectionné figure dans la zone de texte **Nom du travailleur** dans l'onglet **Détail** du connecteur et les informations sur le type de connecteur figurent dans la zone de texte **Type de connecteur**.
- 3 Assurez-vous que le connecteur est lié à l'annuaire Active Directory souhaité en spécifiant cet annuaire dans la zone de texte **Annuaire associé**.
- 4 Entrez le nom de domaine approprié dans la zone de texte **Domaines associés**.
- 5 Sélectionnez l'onglet **AuthAdapters** et activez CertificateAuthAdapter.
- 6 Configurez l'authentification par certificat de la façon appropriée pour votre déploiement.
Reportez-vous à [Configurer l'authentification du certificat dans la gestion des annuaires](#).
- 7 Sélectionnez **Administration > Directories Management > Stratégies**.
- 8 Cliquez sur **Modifier la stratégie par défaut**.
- 9 Ajoutez un certificat aux règles de stratégie et faites-en la première méthode d'authentification.
Le certificat doit être la première méthode d'authentification répertoriée dans la règle de stratégie, sinon l'authentification par certificat échoue.

Créer un lien Active Directory à domaines multiples ou à forêts multiples

En tant qu'administrateur système, vous devez configurer un lien Active Directory à domaines multiples ou à forêts multiples.

Qu'il s'agisse de configurer un lien Active Directory à domaines multiples ou à forêts multiples, la procédure utilisée est essentiellement la même. Pour un lien à forêts multiples, il est nécessaire d'avoir une confiance bidirectionnelle entre tous les domaines applicables.

Prérequis

- Installez un déploiement vRealize Automation distribué avec des équilibres de charge appropriés.
Reportez-vous à *Installation de vRealize Automation 7.3*.
- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.
- Configurez les domaines et forêts Active Directory appropriés pour votre déploiement.

Procédure

- 1 Sélectionnez **Administration > Gestion des répertoires > Répertoires**.
- 2 Cliquez sur **Ajouter un annuaire**.

- 3 Sur la page Ajouter un annuaire, spécifiez le nom du serveur Active Directory dans la zone de texte **Nom de l'annuaire**.
- 4 Sélectionnez l'option **Active Directory (Authentification Windows intégrée)** sous l'en-tête **Nom de l'annuaire**.
- 5 Configurez le connecteur qui synchronise les utilisateurs entre Active Directory et l'annuaire VMware Directories Management dans la section Synchronisation d'annuaires et authentification.

Option	Description
Connecteur de synchronisation	Sélectionnez le connecteur approprié à utiliser avec votre système. Chaque dispositif vRealize Automation contient un connecteur par défaut. Consultez votre administrateur système si vous avez besoin d'aide pour choisir le connecteur approprié.
Authentification	Cliquez sur le bouton radio approprié pour indiquer si le connecteur sélectionné effectue également l'authentification.
Attribut de recherche d'annuaire	Sélectionnez l'attribut de compte approprié contenant le nom d'utilisateur.

Selon la configuration de votre déploiement, un ou plusieurs connecteurs seront disponibles.

- 6 Entrez les informations d'identification de domaine de jonction dans les zones de texte **Nom de domaine**, **Nom de l'utilisateur administrateur de domaine** et **Mot de passe de l'administrateur de domaine**.

Vous pourriez, par exemple, entrer des informations à peu près similaires à ce qui suit : **Nom de domaine** : hs.trcint.com, **Nom de l'utilisateur administrateur de domaine** : devadmin, **Mot de passe de l'administrateur de domaine** : xxxx.

- 7 Dans la section **Détails de l'utilisateur Bind**, entrez les informations d'identification Active Directory appropriées (Authentification Windows intégrée) pour faciliter la synchronisation des annuaires.

Option	Description
UPN de l'utilisateur Bind	Entrez le nom principal d'utilisateur de l'utilisateur qui peut s'authentifier auprès du domaine. Par exemple, UserName@example.com.
Mot de passe du nom unique de liaison	Entrez le mot de passe de l'utilisateur Bind.


- 8 Cliquez sur **Enregistrer et Suivant**.

La page Sélectionnez les domaines apparaît avec la liste des domaines.

- 9 Cochez les cases appropriées pour sélectionner les domaines voulus pour le déploiement de votre système.
- 10 Cliquez sur **Suivant**.
- 11 Vérifiez que les noms d'attributs de l'annuaire Directories Management sont mappés aux attributs Active Directory appropriés.

Si les noms d'attributs de l'annuaire ne sont pas correctement mappés, sélectionnez le bon attribut Active Directory dans le menu déroulant.


- 12 Cliquez sur **Suivant**.


- 13 Cliquez sur  pour sélectionner les groupes que vous souhaitez synchroniser entre Active Directory et l'annuaire.

Lorsque vous ajoutez un groupe Active Directory, si les membres de ce groupe ne figurent pas dans la liste Utilisateurs, ils y sont ajoutés.

Remarque Le système d'authentification utilisateur Directories Management importe les données provenant d'Active Directory lors de l'ajout des groupes et utilisateurs, et la vitesse du système est limitée par les capacités d'Active Directory. Par conséquent, les opérations d'importation peuvent être assez longues, suivant le nombre de groupes et d'utilisateurs à ajouter. Pour minimiser les retards ou problèmes potentiels, limitez le nombre de groupes et d'utilisateurs à ceux requis pour l'opération vRealize Automation. Si les performances de votre système déclinent ou si des erreurs se produisent, fermez toutes les applications inutiles et assurez-vous que votre système dispose d'une mémoire suffisante attribuée à Active Directory. Si les problèmes persistent, augmentez cette allocation de mémoire selon les besoins. Pour les systèmes comportant un nombre important d'utilisateurs et de groupes, vous pouvez allouer à Active Directory jusqu'à 24 Go de mémoire.

- 14 Cliquez sur **Suivant**.

- 15 Cliquez sur  pour ajouter des utilisateurs supplémentaires. Par exemple, effectuez la saisie sous la forme **CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com**.

Pour exclure des utilisateurs, cliquez sur  afin de créer un filtre permettant d'exclure certains types d'utilisateurs. Vous pouvez sélectionner un attribut d'utilisateur à filtrer, la règle de requête et sa valeur.

- 16 Cliquez sur **Suivant**.

- 17 Examinez la page pour voir combien d'utilisateurs et de groupes sont synchronisés avec l'annuaire.

Si vous souhaitez apporter des modifications aux utilisateurs et aux groupes, cliquez sur les liens Modifier.

- 18 Cliquez sur **Transférer vers Workspace** pour lancer la synchronisation avec l'annuaire.

Suivant

Configuration de groupes et de rôles d'utilisateur

Les administrateurs de locataires créent des groupes d'activité et des groupes personnalisés, et octroient des droits d'accès d'utilisateur à la console vRealize Automation.

Attribuer des rôles à des utilisateurs ou des groupes du répertoire

Les administrateurs de locataires octroient aux utilisateurs des droits d'accès en attribuant des rôles aux utilisateurs ou aux groupes.

Pour autoriser des utilisateurs ou groupes à modifier et à déclencher un pipeline, vous devez attribuer des autorisations à ces utilisateurs et groupes. Lorsque vous attribuez aux utilisateurs et groupes le rôle de gestionnaire de version, ils peuvent modifier et déclencher le pipeline. Lorsque vous attribuez aux utilisateurs et groupes le rôle d'ingénieur de version, ils peuvent déclencher le pipeline. Pour plus d'informations, reportez-vous au guide *Utilisation de vRealize Code Stream*.

Prérequis

Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

1 Sélectionnez **Administration > Utilisateurs et groupes > Utilisateurs et groupes de répertoires**.

2 Entrez un nom d'utilisateur ou de groupe dans la case **Recherche** et appuyez sur Entrée.

N'utilisez pas le symbole @, ni les caractères de barre oblique inverse (\) ou de barre oblique (/) dans un nom. Vous pouvez optimiser votre recherche en tapant le nom d'utilisateur ou de groupe entier dans le formulaire user@domain.

3 Cliquez sur le nom de l'utilisateur ou du groupe auquel vous souhaitez attribuer des rôles.

4 Sélectionnez un ou plusieurs rôles dans la liste Ajouter des rôles à cet utilisateur.

La liste Autorisations accordées par rôles sélectionnés indique les autorités spécifiques que vous accordez.

5 (Facultatif) Cliquez sur **Suivant** pour afficher plus d'informations sur l'utilisateur ou le groupe.

6 Sur la page **Détails de l'utilisateur**, dans l'onglet **Général**, faites défiler la liste des rôles pour ajouter l'utilisateur.

a Pour autoriser l'utilisateur à modifier et à déclencher un pipeline, cochez la case **Gestionnaire de version**.

b Pour autoriser l'utilisateur à déclencher un pipeline, cochez la case **Ingénieur de version**.

7 Cliquez sur **Mise à jour**.

Les utilisateurs connectés dans la console de vRealize Automation doivent se déconnecter et se reconnecter à la console de vRealize Automation pour pouvoir accéder aux pages pour lesquelles ils ont obtenu l'accès.

Suivant

Vous pouvez éventuellement créer vos propres groupes personnalisés à partir des utilisateurs et des groupes de vos connexions Active Directory. Reportez-vous à [Créer un groupe personnalisé](#).

Créer un groupe personnalisé

Les administrateurs de locataires peuvent créer des groupes personnalisés en combinant d'autres groupes personnalisés, des groupes de magasins d'identités et d'autres utilisateurs individuels de magasins d'identités. Les groupes personnalisés fournissent un contrôle plus granulaire de l'accès à vRealize Automation qu'à des groupes d'activités qui correspondent à un secteur d'activité, à un service ou à une autre unité d'organisation.

Les groupes personnalisés permettent d'accorder des droits d'accès pour des tâches sur une base plus précise que les attributions de groupe vRealize Automation standard. Par exemple, vous pouvez créer un groupe personnalisé pour permettre aux administrateurs locataires de contrôler qui dispose d'autorisations spécifiques dans le locataire.

Vous pouvez attribuer des rôles à votre groupe personnalisé, mais cela n'est pas nécessaire dans tous les cas. Par exemple, vous pouvez créer un groupe personnalisé appelé Approbateurs de spécifications de machines à utiliser pour toutes les approbations préalables de machine. Vous pouvez également créer des groupes personnalisés à mapper à vos groupes d'activité de façon que vous puissiez gérer tous les groupes dans un seul emplacement. Dans ce cas, il n'est pas nécessaire d'attribuer des rôles.

Prérequis

Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

- 1 Sélectionnez **Administration > Utilisateurs et groupes > Groupes personnalisés**.
- 2 Cliquez sur l'icône **Ajouter** (+).
- 3 Entrez un nom de groupe dans la zone de texte **Nom du nouveau groupe**.
Les noms des groupes personnalisés ne peuvent pas contenir un point virgule (;) suivi du signe égal (=).
- 4 (Facultatif) Entrez une description dans la zone de texte **Description du nouveau groupe**.
- 5 Sélectionnez un ou plusieurs rôles dans la liste **Ajouter des rôles à ce groupe**.
La liste **Autorisations accordées par rôles sélectionnés** indique les autorités spécifiques que vous accordez.
- 6 Cliquez sur **Suivant**.
- 7 Ajoutez des utilisateurs et des groupes pour créer votre groupe personnalisé.
 - a Entrez un nom d'utilisateur ou de groupe dans la case **Recherche** et appuyez sur Entrée.
N'utilisez pas le symbole @, ni les caractères de barre oblique inverse (\) ou de barre oblique (/) dans un nom. Vous pouvez optimiser votre recherche en tapant le nom d'utilisateur ou de groupe entier dans le formulaire user@domain.
 - b Sélectionnez l'utilisateur ou le groupe à ajouter à votre groupe personnalisé.
- 8 Cliquez sur **Ajouter**.

Les utilisateurs connectés dans la console de vRealize Automation doivent se déconnecter et se reconnecter à la console de vRealize Automation pour pouvoir accéder aux pages pour lesquelles ils ont obtenu l'accès.

Créer un groupe d'activité

Les groupes d'activité permettent d'associer un ensemble de services et de ressources à un ensemble d'utilisateurs. Ces groupes correspondent souvent à un secteur d'activité, à un département ou à une autre unité d'organisation. Créez un groupe d'activité afin de configurer des réservations et d'autoriser des utilisateurs à provisionner des éléments du catalogue de services pour les membres du groupe d'activité.

Pour ajouter plusieurs utilisateurs à un rôle de groupe d'activité, vous pouvez ajouter plusieurs utilisateurs individuellement, ou vous pouvez ajouter plusieurs utilisateurs à la fois en ajoutant un groupe de magasin d'identité ou un groupe personnalisé à un rôle. Par exemple, vous pouvez créer un groupe personnalisé Équipe de support commercial et ajouter ce groupe au rôle de support. Vous pouvez également utiliser des groupes d'utilisateurs de magasin d'identité existants. Les utilisateurs et groupes que vous choisissez doivent être valides dans le magasin d'identité.

Pour prendre en charge l'intégration vCloud Director, les membres du groupe d'activité vRealize Automation doivent également être membres de l'organisation vCloud Director.

Après qu'un administrateur de locataire a créé le groupe d'activité, le gestionnaire de ce groupe possède l'autorisation de modifier l'adresse e-mail du gestionnaire et les membres du groupe. L'administrateur de locataire, quant à lui, peut modifier toutes les options.

Pour ce faire, IaaS doit être installé et configuré.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.
- Si vous voulez ajouter des machines créées par des membres du groupe d'activité à une unité d'organisation Active Directory particulière, configurez la stratégie Active Directory. Reportez-vous à [Créer une stratégie Active Directory](#). Vous pouvez appliquer la stratégie lors de la création du groupe d'activité ou l'ajouter ultérieurement.
- Si vous voulez fournir un préfixe de machine par défaut pour le groupe qui est ajouté au début des noms de machines provisionnées, demandez un préfixe à un administrateur Fabric. Reportez-vous à [Configurer des préfixes de machines](#). Les préfixes de machine ne s'appliquent pas aux demandes XaaS.

Procédure

- 1 Sélectionnez **Administration > Utilisateurs et groupes > Groupes d'activité**.
- 2 Cliquez sur l'icône **Nouveau (+)**.

3 Configurez les détails du groupe d'activité.

Option	Description
Nom	Entrez le nom du groupe d'activité.
Description	Entrez la description.
Envoyer les e-mails de gestionnaire à	Entrez une ou plusieurs adresses e-mail des utilisateurs qui doivent recevoir des notifications d'alerte de capacité. Les adresses e-mail alias ne sont pas prises en charge, chaque adresse e-mail doit être celle d'un utilisateur spécifique. Séparez les entrées multiples par une virgule. Par exemple, JoeAdmin@mycompany.com,WeiMgr@mycompany.com.
Stratégie Active Directory	Sélectionnez la stratégie Active Directory par défaut pour le groupe d'activité.

4 Ajoutez des propriétés personnalisées.

5 Entrez un nom d'utilisateur ou un nom de groupe d'utilisateurs personnalisé, puis appuyez sur Entrée.

Vous pouvez ajouter au groupe d'activité un ou plusieurs individus, ou des groupes d'utilisateurs personnalisés. Vous pouvez spécifier les utilisateurs maintenant ou créer des groupes d'activité vides à remplir ultérieurement.

Option	Description
Rôle de gestionnaire de groupes	Peut créer des droits d'accès et attribuer des stratégies d'approbation au groupe
Rôle de support	Peut demander et gérer des éléments du catalogue de services au nom des autres membres du groupe d'activité
Rôle avec accès partagé	Peut utiliser et exécuter des actions sur les ressources déployées par d'autres membres du groupe d'activité.
Rôle d'utilisateur	Peut demander des éléments du catalogue de services pour lesquels il possède un droit d'accès

6 Cliquez sur **Suivant**.

7 Configurez les options d'infrastructure par défaut.

Option	Description
Préfixe de machine par défaut	Sélectionnez un préfixe de machine préconfiguré pour le groupe d'activité. Ce préfixe est utilisé par les Blueprints de machine. Si le Blueprint utilise le préfixe par défaut et si vous ne le fournissez pas ici, un préfixe de machine est créé en fonction du nom du groupe d'activité. Il est préférable d'indiquer un préfixe par défaut. Vous pouvez toujours configurer des Blueprints avec des préfixes spécifiques ou autoriser les utilisateurs du catalogue de services à le remplacer lorsqu'ils demandent un Blueprint. Les Blueprints XaaS n'utilisent pas de préfixes de machine par défaut. Si vous configurez un préfixe et que vous autorisez un Blueprint XaaS à accéder à ce groupe d'activité, le provisionnement d'une machine XaaS n'est aucunement affecté.
Conteneur Active Directory	Entrez un conteneur Active Directory. Cette option s'applique uniquement au provisionnement WIM. D'autres méthodes de provisionnement exigent une configuration supplémentaire afin de joindre les machines provisionnées à un conteneur AD.

8 Cliquez sur **Ajouter**.

Les administrateurs Fabric peuvent allouer des ressources au groupe d'activité en créant une réservation. Les gestionnaires du groupe d'activité peuvent créer des droits d'accès pour les membres du groupe d'activité.

Suivant

- Créez une réservation pour votre groupe d'activité en fonction de l'emplacement auquel ce groupe provisionne les machines. Reportez-vous à [Choisir un scénario de réservation](#).
- Si les éléments du catalogue sont publiés et que les services existent, vous pouvez créer un droit d'accès pour les membres du groupe d'activité. Reportez-vous à [Autoriser des utilisateurs à accéder à des services, des éléments de catalogue et des actions](#).

Dépannage des problèmes de baisse de performances lors de l'affichage des membres de groupe

Les membres du groupe d'activité ou du groupe personnalisé mettent du temps à apparaître lors de l'affichage des détails du groupe.

Problème

Lorsque vous affichez des informations utilisateur dans des environnements comportant un grand nombre d'utilisateurs, le chargement des noms d'utilisateurs dans l'interface utilisateur est long.

Cause

Cette baisse de performances survient dans des environnements dans lesquels Active Directory est volumineux.

Solution

- ◆ Pour réduire la charge de travail qu'induit cette récupération, utilisez les groupes Active Directory ou des groupes personnalisés chaque fois que possible plutôt que d'ajouter individuellement des centaines de noms de membres.

Créer des locataires supplémentaires

En tant qu'administrateur système, vous pouvez créer des locataires vRealize Automation supplémentaires, afin que les utilisateurs puissent accéder aux applications et ressources nécessaires à leurs attributions professionnelles.

Un locataire est un groupe d'utilisateurs disposant de privilèges spécifiques et qui travaillent dans une instance logicielle. Généralement, un locataire vRealize Automation est créé par défaut lors de l'installation du système et de la configuration initiale. Ultérieurement, les administrateurs peuvent créer d'autres locataires afin que les utilisateurs puissent se connecter et accomplir leur travail. Les administrateurs peuvent créer autant de locataires que nécessaire au fonctionnement du système. Ce faisant, ils doivent spécifier une configuration de base, telle que le nom, l'URL de connexion, les utilisateurs locaux et les administrateurs. Après la configuration des informations de base relatives aux

locataires, l'administrateur de locataire doit se connecter et configurer une connexion Active Directory adaptée à l'aide de la fonctionnalité Directories Management, dans l'onglet Administration de la console de vRealize Automation. De plus, l'administrateur de locataire peut appliquer des informations de personnalisation aux locataires.

Prérequis

Connectez-vous à la console de vRealize Automation en tant qu'**administrateur système**.

Procédure

1 Spécifier les informations d'un locataire

La première étape de configuration d'un locataire consiste à nommer le nouveau locataire et à l'ajouter à vRealize Automation, puis à créer l'URL d'accès spécifique au locataire.

2 Configurer des utilisateurs locaux

L'administrateur système vRealize Automation doit configurer les utilisateurs locaux de chaque locataire concerné.

3 Nommer des administrateurs

Vous pouvez nommer un ou plusieurs administrateurs de locataire et administrateurs IaaS à partir des magasins d'identités que vous avez configurés pour un locataire.

Spécifier les informations d'un locataire

La première étape de configuration d'un locataire consiste à nommer le nouveau locataire et à l'ajouter à vRealize Automation, puis à créer l'URL d'accès spécifique au locataire.

Prérequis

Connectez-vous à la console de vRealize Automation en tant qu'**administrateur système**.

Procédure

1 Sélectionnez **Administration > Locataires**.

2 Cliquez sur l'icône **Nouveau (+)**.

3 Entrez un nom dans la zone de texte **Nom**.

4 (Facultatif) Entrez une description dans la zone de texte **Description**.

5 Entrez un identifiant unique pour le propriétaire dans la zone de texte **Nom d'URL**.

Ce jeton d'URL est utilisé pour ajouter un identifiant propre au locataire à l'URL de la console vRealize Automation.

Par exemple, entrez **mytenant** pour créer l'URL `https://vrealize-appliance-hostname.domain.name/vcac/org/mytenant`.

Remarque L'URL du locataire doit utiliser exclusivement des caractères en minuscule uniquement dans vRealize Automation 7.0 et 7.1.

6 (Facultatif) Entrez une adresse e-mail dans la zone de texte **e-mail de contact**.

7 Cliquez sur **Envoyer et Suivant**.

Configurer des utilisateurs locaux

L'administrateur système vRealize Automation doit configurer les utilisateurs locaux de chaque locataire concerné.

Après qu'un administrateur a créé les informations générales d'un locataire, l'onglet Utilisateurs locaux est activé et l'administrateur peut désigner les utilisateurs qui disposent d'un droit d'accès au locataire. Une fois la configuration du locataire terminée, les utilisateurs locaux peuvent se connecter à leurs locataires respectifs pour terminer les attributions de travail.

Remarque Après l'ajout d'un utilisateur, vous ne pouvez pas modifier sa configuration. Si vous devez apporter une modification à la configuration de l'utilisateur, vous devez supprimer celui-ci et le recréer.

Procédure

- 1 Dans l'onglet Utilisateurs locaux, cliquez sur le bouton **Ajouter**.
- 2 Dans la boîte de dialogue Détails de l'utilisateur, entrez les noms et prénoms des utilisateurs dans les champs **Prénom** et **Nom**.
- 3 Dans le champ **E-mail**, entrez l'adresse e-mail de l'utilisateur.
- 4 Dans les champs **Nom d'utilisateur** et **Mot de passe**, entrez l'ID d'utilisateur et le mot de passe.
- 5 Cliquez sur le bouton **Ajouter**.
- 6 Répétez ces étapes si nécessaire pour tous les utilisateurs locaux du locataire.

Les utilisateurs locaux spécifiés du locataire sont désormais créés.

Nommer des administrateurs

Vous pouvez nommer un ou plusieurs administrateurs de locataire et administrateurs laaS à partir des magasins d'identités que vous avez configurés pour un locataire.

Les administrateurs de locataire sont responsables de la configuration de la personnalisation spécifique à un locataire ainsi que de la gestion des magasins d'identités, des utilisateurs, groupes, droit d'accès et Blueprints partagés dans le cadre de leur locataire. Les administrateurs laaS sont responsables de la configuration des points de terminaison sources de l'infrastructure dans laaS, de la nomination d'administrateurs Fabric et de la surveillance des journaux laaS.

Prérequis

- Avant de nommer des administrateurs laaS, installez laaS. Pour plus d'informations sur l'installation d'laaS, reportez-vous à *Installation de vRealize Automation 7.3*.

Procédure

- 1 Entrez le nom d'un utilisateur ou groupe dans la zone de texte **Administrateurs de locataire** et appuyez sur Entrée.

Pour des résultats plus rapides, entrez le nom d'utilisateur ou de groupe entier, par exemple myAdmins@mycompany.domain. Répétez cette étape pour nommer des administrateurs de locataire supplémentaires.

- 2 Si vous avez installé IaaS, entrez le nom d'un utilisateur ou groupe dans la zone de texte **Administrateurs IaaS** et appuyez sur Entrée.

Pour des résultats plus rapides, entrez le nom d'utilisateur ou de groupe entier, par exemple IaaSAdmins@mycompany.domain. Répétez cette étape pour nommer des administrateurs d'infrastructure supplémentaires.

- 3 Cliquez sur **Ajouter**.

Suppression d'un locataire

Un administrateur système peut supprimer tous les locataires indésirables de vRealize Automation.

Si vous supprimez un locataire, celui-ci sera supprimé immédiatement de l'interface vRealize Automation, mais la suppression totale du locataire de votre déploiement peut prendre quelques heures. Si vous supprimez un locataire et que vous souhaitez créer un locataire avec la même URL, attendez quelques heures que la suppression soit terminée.

Prérequis

Connectez-vous à la console de vRealize Automation en tant qu'**administrateur système**.

Procédure

- 1 Sélectionnez **Administration > Locataires**.
- 2 Sélectionnez le locataire que vous souhaitez supprimer.

Ne cliquez pas sur son nom pour le sélectionner, car cela l'ouvrirait pour modification.

- 3 Cliquez sur **Supprimer**.

Le locataire est supprimé de votre déploiement de vRealize Automation.

(Facultatif) Configuration de la personnalisation

vRealize Automation vous permet d'appliquer une personnalisation aux pages de connexion de locataire et d'application.

La personnalisation peut inclure des couleurs de texte et d'arrière-plan, des logos d'entreprise, un nom d'entreprise, des stratégies de confidentialité, des avis de droits d'auteur et d'autres informations pertinentes que vous souhaitez voir figurer sur les pages de connexion de locataire ou d'application.

Personnalisation de la page de connexion du locataire

Utilisez la page Personnalisation de l'écran de connexion pour appliquer une personnalisation à vos pages de connexion de locataire vRealize Automation.

Vous pouvez utiliser la personnalisation par défaut de vRealize Automation sur vos pages de connexion de locataire ou vous pouvez configurer une personnalisation à l'aide de la page Personnalisation de l'écran de connexion. Notez que la personnalisation s'applique de la même manière à toutes vos applications de locataire.

Cette page vous permet de configurer la personnalisation sur toutes les pages de connexion de locataire.

La page Personnalisation de l'écran de connexion affiche la personnalisation de connexion de locataire actuellement implémentée dans le volet Aperçu.

Remarque Après l'enregistrement de la nouvelle personnalisation de la page de connexion de locataire, il peut s'écouler jusqu'à cinq minutes avant qu'elle ne devienne visible sur toutes les pages de connexion.

Prérequis

Pour utiliser un logo personnalisé ou une autre image incluant vos informations de marque, vous devez disposer des fichiers appropriés.

Procédure

- 1 Connectez-vous à vRealize Automation en tant qu'administrateur système ou administrateur de locataires.
- 2 Cliquez sur l'onglet **Administration**.
- 3 Sélectionnez les effets visuels souhaités à l'aide des cases à cocher sous le titre Effets.
Tous les effets sont facultatifs.
- 4 Sélectionnez **Personnalisation > Personnalisation de l'écran de connexion**
- 5 Cliquez sur **Télécharger** sous le champ Logo, puis accédez au dossier approprié et sélectionnez un fichier d'image de logo.
- 6 Si vous le souhaitez, cliquez sur **Télécharger** sous le champ Image (facultatif), puis accédez au dossier approprié, puis sélectionnez un fichier d'image supplémentaire.
- 7 Si vous le souhaitez, entrez les codes hexadécimaux appropriés dans les champs **Couleur d'arrière-plan**, **Couleur de cartouche de titre**, **Couleur d'arrière-plan du bouton de connexion** et **Couleur de premier plan du bouton de connexion**.
Recherchez sur Internet une liste des codes couleur hexadécimaux si nécessaire.
- 8 Cliquez sur **Enregistrer** pour appliquer vos paramètres.

Les utilisateurs du locataire voient la personnalisation sur leurs pages de connexion.

Personnalisation des applications du locataire

Utilisez la page Personnalisation d'application pour appliquer une personnalisation à des applications de locataire vRealize Automation.

Vous pouvez utiliser la personnalisation par défaut de vRealize Automation sur vos applications d'utilisateur ou vous pouvez configurer une personnalisation à l'aide de la page Personnalisation d'application. Cette page vous permet de configurer la personnalisation sur l'en-tête et le pied de page des pages d'application. Notez que la personnalisation s'applique de la même manière à toutes vos applications d'utilisateur.

La page Personnalisation d'application affiche en bas de la page la personnalisation de l'en-tête ou du pied de page actuellement implémentée.

Prérequis

Si vous souhaitez utiliser un logo personnalisé avec votre personnalisation, vous devez avoir accès au fichier d'image du logo.

Procédure

- 1 Connectez-vous à vRealize Automation en tant qu'administrateur système ou administrateur de locataires.
- 2 Cliquez sur l'onglet **Administration**.
- 3 Sélectionnez **Personnalisation > Personnalisation d'application**
- 4 Cliquez sur l'onglet **En-tête** s'il n'est pas déjà actif.
- 5 Si vous souhaitez utiliser la personnalisation vRealize Automation par défaut, cliquez sur la case à cocher **Utiliser le réglage par défaut**.
- 6 Pour implémenter la personnalisation, effectuez les sélections appropriées dans les champs des onglets **En-tête** et **Pied de page**.
 - a Cliquez sur le bouton **Parcourir** dans le champ **Logo de l'en-tête**, puis accédez au dossier approprié et sélectionnez un fichier d'image de logo.
 - b Tapez le nom de société approprié dans le champ **Nom de la société**.
Le nom spécifié s'affiche lorsque l'utilisateur fait passer le pointeur de la souris au-dessus du logo.
 - c Tapez le nom approprié dans le champ **Nom du produit**.
Le nom que vous entrez ici s'affiche dans l'en-tête de l'application, près du logo.
 - d Entrez le code couleur hexadécimal approprié pour la couleur d'arrière-plan du périmètre de l'application dans le champ **Couleur hex de l'arrière-plan**.
Recherchez sur Internet une liste des codes couleur hexadécimaux si nécessaire.

- e Entrez le code hexadécimal approprié pour la couleur du texte dans le champ **Couleur hex du texte**.

Recherchez sur Internet une liste des codes couleur de texte hexadécimaux si nécessaire.

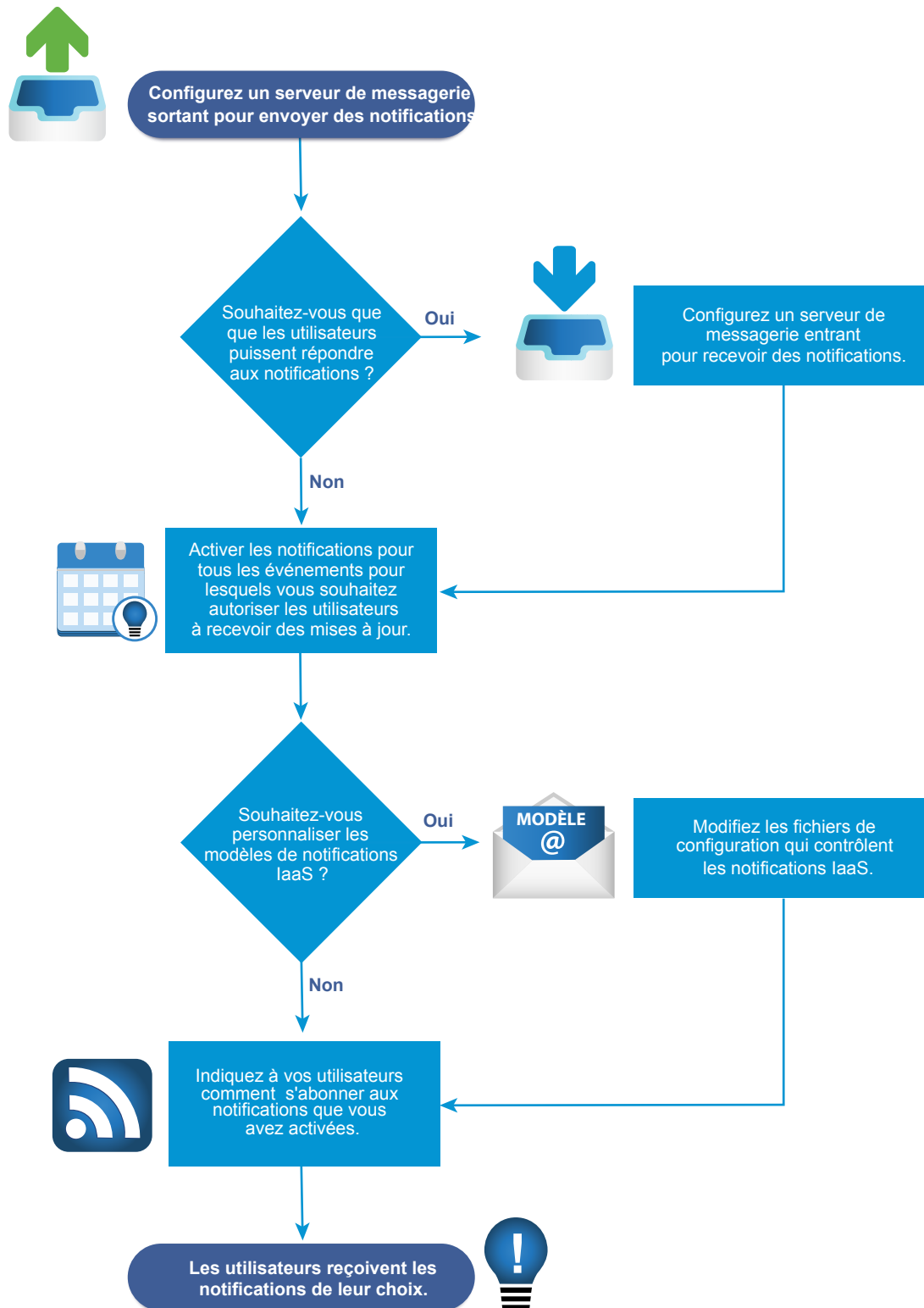
- f Cliquez sur **Suivant** pour activer l'onglet Pied de page.
- g Tapez la déclaration souhaitée dans le champ **Copyright**.
- h Tapez le lien vers la déclaration de la politique de confidentialité de votre entreprise dans le champ **Lien de Déclaration de confidentialité**.
- i Tapez les informations de contact souhaitées pour la société dans le champ **Lien de Contact**.

- 7 Cliquez sur **Mettre à jour** pour implémenter votre configuration de personnalisation.

Les utilisateurs du locataire voient la personnalisation sur leurs pages d'application.

(Facultatif) Liste de contrôle de la configuration des notifications

Vous pouvez configurer vRealize Automation pour envoyer aux utilisateurs des notifications lorsque des événements spécifiques se produisent. Les utilisateurs peuvent choisir à quelles notifications ils souhaitent s'abonner, mais ils peuvent uniquement sélectionner les événements que vous activez comme déclencheurs de notification.



La liste de contrôle Configuration de notifications fournit une présentation de haut niveau de la séquence d'étapes requises pour configurer des notifications et fournit des liens vers des points de décision ou des instructions détaillées pour chaque étape.

Tableau 2-10. Liste de contrôle de la configuration des notifications

Tâche	Rôle requis	Détails
<input type="checkbox"/> Configurer un serveur de messagerie sortant pour envoyer des notifications.	<ul style="list-style-type: none"> ■ Les administrateurs système configurent les serveurs globaux par défaut. ■ Les administrateurs de locataires configurent des serveurs pour leurs locataires. 	<p>Pour configurer un serveur la première fois pour votre locataire, reportez-vous à Ajouter un serveur de messagerie sortant spécifique à un locataire. Si vous devez remplacer un serveur global par défaut, reportez-vous à Remplacer un serveur de messagerie sortant par défaut du système.</p> <p>Pour configurer des serveurs par défaut globaux pour tous les locataires, reportez-vous à Créer un serveur de messagerie sortant global.</p>
<input type="checkbox"/> (Facultatif) Configurer un serveur de messagerie entrant afin que les utilisateurs puissent exécuter des tâches en répondant à des notifications.	<ul style="list-style-type: none"> ■ Les administrateurs système configurent les serveurs globaux par défaut. ■ Les administrateurs de locataires configurent des serveurs pour leurs locataires. 	<p>Pour configurer un serveur la première fois pour votre locataire, reportez-vous à Ajouter un serveur de messagerie entrant spécifique à un locataire.</p> <p>Si vous devez remplacer un serveur global par défaut, reportez-vous à Remplacer un serveur de messagerie entrant par défaut du système.</p> <p>Pour configurer un serveur par défaut global pour tous les locataires, reportez-vous à Créer un serveur de messagerie entrant global.</p>
<input type="checkbox"/> (Facultatif) Spécifier quand une notification par e-mail doit être envoyée avant la date d'expiration d'une machine.	Administrateur système	Reportez-vous à Personnaliser la date de notification par e-mail de l'expiration d'une machine .
<input type="checkbox"/> Sélectionner les événements vRealize Automation pour déclencher les notifications utilisateur. Les utilisateurs peuvent uniquement s'abonner à des notifications pour des événements que vous activez comme déclencheurs de notification.	Administrateur de locataire	Reportez-vous à Configurer des notifications .

Tableau 2-10. Liste de contrôle de la configuration des notifications (suite)

Tâche	Rôle requis	Détails
<input type="checkbox"/> (Facultatif) Configurer les modèles pour les notifications envoyées aux propriétaires de machines concernant des événements qui impliquent leurs machines, par exemple l'expiration du bail.	Toute personne ayant accès à l'annuaire \Temp\ates sous l'annuaire d'installation du serveur vRealize Automation (généralement %SystemDrive%\Program Files\VMware\VCAServer) peut configurer les modèles de ces e-mails de notification.	Reportez-vous à Configuration de modèles pour les e-mails IaaS automatiques .
<input type="checkbox"/> Fournir à vos utilisateurs des instructions sur l'abonnement aux notifications que vous avez activées. Ils peuvent choisir de s'abonner uniquement aux notifications pertinentes pour leur rôle.	Tous les utilisateurs	Reportez-vous à S'abonner aux notifications .

Configuration de serveurs de messagerie globaux pour les notifications

Les administrateurs de locataire peuvent ajouter des serveurs de messagerie dans le cadre de la configuration de notifications pour leurs propres locataires. En tant qu'administrateur système, vous pouvez configurer des serveurs de messagerie entrants et sortants globaux qui apparaissent à tous les locataires comme paramètres par défaut. Si les administrateurs de locataire ne remplacent pas ces paramètres avant d'activer les notifications, vRealize Automation utilise les serveurs de messagerie globaux configurés.

Créer un serveur de messagerie entrant global

Les administrateurs système créent un serveur de messagerie entrant global pour gérer les e-mails de notification entrants, comme les réponses aux approbations. Vous ne pouvez créer qu'un seul serveur entrant, qui apparaît comme le serveur par défaut pour tous les locataires. Si les administrateurs de locataire ne remplacent pas ces paramètres avant d'activer les notifications, vRealize Automation utilise le serveur de messagerie global configuré.

Prérequis

Connectez-vous à la console de vRealize Automation en tant qu'**administrateur système**.

Procédure

- 1 Sélectionnez **Administration > Serveurs de messagerie**.
- 2 Cliquez sur l'icône **Ajouter (+)**.

- 3 Sélectionnez **Messagerie – Entrante**.
- 4 Cliquez sur **OK**.
- 5 Entrez un nom dans la zone de texte **Nom**.
- 6 (Facultatif) Entrez une description dans la zone de texte **Description**.
- 7 (Facultatif) Cochez la case **SSL** pour utiliser SSL pour la sécurité.
- 8 Choisissez un protocole de serveur.
- 9 Saisissez le nom du serveur dans la zone de texte **Nom du serveur**.
- 10 Tapez le numéro de port du serveur dans la zone de texte **Port du serveur**.
- 11 Tapez le nom du dossier des e-mails dans la zone de texte **Nom de dossier**.
Cette option est requise uniquement si vous choisissez le protocole de serveur IMAP.
- 12 Entrez un nom d'utilisateur dans la zone de texte **Nom d'utilisateur**.
- 13 Entrez un mot de passe dans la zone de texte **Mot de passe**.
- 14 Tapez l'adresse électronique à laquelle les utilisateurs de vRealize Automation peuvent répondre dans la zone de texte **Adresse électronique**.
- 15 (Facultatif) Sélectionnez **Supprimer du serveur** pour supprimer du serveur tous les e-mails traités récupérés par le service de notification.
- 16 Choisissez si vRealize Automation peut accepter des certificats autosignés du serveur de messagerie.
- 17 Cliquez sur **Tester la connexion**.
- 18 Cliquez sur **Ajouter**.

Créer un serveur de messagerie sortant global

Les administrateurs système créent un serveur de messagerie sortant global pour gérer les e-mails de notification sortants. Vous ne pouvez créer qu'un seul serveur sortant, qui apparaît comme le serveur par défaut pour tous les locataires. Si les administrateurs de locataire ne remplacent pas ces paramètres avant d'activer les notifications, vRealize Automation utilise le serveur de messagerie global configuré.

Prérequis

Connectez-vous à la console de vRealize Automation en tant qu'**administrateur système**.

Procédure

- 1 Sélectionnez **Administration > Serveurs de messagerie**.
- 2 Cliquez sur l'icône **Ajouter (+)**.
- 3 Sélectionnez **Messagerie – Sortante**.
- 4 Cliquez sur **OK**.
- 5 Entrez un nom dans la zone de texte **Nom**.

- 6 (Facultatif) Entrez une description dans la zone de texte **Description**.
- 7 Saisissez le nom du serveur dans la zone de texte **Nom du serveur**.
- 8 Choisissez une méthode de chiffrement.
 - Cliquez sur **Utiliser SSL**.
 - Cliquez sur **Utiliser TLS**.
 - Cliquez sur **Aucune** pour envoyer des communications non chiffrées.
- 9 Tapez le numéro de port du serveur dans la zone de texte **Port du serveur**.
- 10 (Facultatif) Cochez la case **Requise** si le serveur requiert une authentification.
 - a Tapez un nom d'utilisateur dans la zone de texte **Nom d'utilisateur**.
 - b Tapez un mot de passe dans la zone de texte **Mot de passe**.
- 11 Tapez l'adresse électronique devant s'afficher pour l'expéditeur de vRealize Automation dans la zone de texte **Adresse de l'expéditeur**.

 Cette adresse électronique correspond au nom d'utilisateur et au mot de passe que vous avez fournis.
- 12 Choisissez si vRealize Automation peut accepter des certificats autosignés du serveur de messagerie.
- 13 Cliquez sur **Tester la connexion**.
- 14 Cliquez sur **Ajouter**.

Ajouter un serveur de messagerie sortant spécifique à un locataire

Les administrateurs de locataire peuvent ajouter un serveur de messagerie sortant afin d'envoyer des notifications concernant des éléments de travail à réaliser comme des approbations.

Chaque propriétaire ne peut avoir qu'un serveur de messagerie sortant. Si votre administrateur système a déjà configuré un serveur de messagerie sortant, reportez-vous à la section [Remplacer un serveur de messagerie sortant par défaut du système](#).

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.
- Si le serveur de messagerie exige une authentification, l'utilisateur spécifié doit se trouver dans un magasin d'identités et dans le groupe d'activité.

Procédure

- 1 Sélectionnez **Administration > Notifications > Serveurs de messagerie**.
- 2 Cliquez sur l'icône **Ajouter (+)**.
- 3 Sélectionnez **Messagerie – Sortante**.
- 4 Cliquez sur **OK**.

- 5 Entrez un nom dans la zone de texte **Nom**.
- 6 (Facultatif) Entrez une description dans la zone de texte **Description**.
- 7 Saisissez le nom du serveur dans la zone de texte **Nom du serveur**.
- 8 Choisissez une méthode de chiffrement.
 - Cliquez sur **Utiliser SSL**.
 - Cliquez sur **Utiliser TLS**.
 - Cliquez sur **Aucune** pour envoyer des communications non chiffrées.
- 9 Tapez le numéro de port du serveur dans la zone de texte **Port du serveur**.
- 10 (Facultatif) Cochez la case **Requise** si le serveur requiert une authentification.
 - a Tapez un nom d'utilisateur dans la zone de texte **Nom d'utilisateur**.
 - b Tapez un mot de passe dans la zone de texte **Mot de passe**.
- 11 Tapez l'adresse électronique devant s'afficher pour l'expéditeur de vRealize Automation dans la zone de texte **Adresse de l'expéditeur**.

Cette adresse électronique correspond au nom d'utilisateur et au mot de passe que vous avez fournis.
- 12 Choisissez si vRealize Automation peut accepter des certificats autosignés du serveur de messagerie.

Cette option est disponible uniquement si vous avez activé le chiffrement.

 - Cliquez sur **Oui** pour accepter les certificats autosignés.
 - Cliquez sur **Non** pour rejeter les certificats autosignés.
- 13 Cliquez sur **Tester la connexion**.
- 14 Cliquez sur **Ajouter**.

Ajouter un serveur de messagerie entrant spécifique à un locataire

Les administrateurs de locataire peuvent ajouter un serveur de messagerie entrant de sorte que les utilisateurs puissent répondre aux notifications concernant des éléments de travail à réaliser comme les approbations.

Chaque propriétaire ne peut avoir qu'un serveur de messagerie entrant. Si votre administrateur système a déjà configuré un serveur de messagerie entrant, reportez-vous à la section [Remplacer un serveur de messagerie entrant par défaut du système](#).

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.
- Vérifiez que l'utilisateur spécifié se trouve dans un magasin d'identités et dans le groupe d'activité.

Procédure

- 1 Sélectionnez **Administration > Notifications > Serveurs de messagerie**.
- 2 Cliquez sur l'icône **Ajouter (+)**.
- 3 Sélectionnez **Messagerie entrante**, puis cliquez sur **OK**.
- 4 Configurez les options suivantes du serveur de messagerie entrant.

Option	Action
Nom	Entrez un nom pour le serveur de messagerie entrant.
Description	Entrez une description du serveur de messagerie entrant.
Sécurité	Sélectionnez la case à cocher Utiliser SSL .
Protocole	Choisissez un protocole de serveur.
Nom du serveur	Entrez le nom du serveur.
Port du serveur	Entrez le numéro de port du serveur.

- 5 Tapez le nom du dossier des e-mails dans la zone de texte **Nom de dossier**.
Cette option est requise uniquement si vous choisissez le protocole de serveur IMAP.
- 6 Entrez un nom d'utilisateur dans la zone de texte **Nom d'utilisateur**.
- 7 Entrez un mot de passe dans la zone de texte **Mot de passe**.
- 8 Tapez l'adresse électronique à laquelle les utilisateurs de vRealize Automation peuvent répondre dans la zone de texte **Adresse électronique**.
- 9 (Facultatif) Sélectionnez **Supprimer du serveur** pour supprimer du serveur tous les e-mails traités récupérés par le service de notification.
- 10 Choisissez si vRealize Automation peut accepter des certificats autosignés du serveur de messagerie.
Cette option est disponible uniquement si vous avez activé le chiffrement.
 - Cliquez sur **Oui** pour accepter les certificats autosignés.
 - Cliquez sur **Non** pour rejeter les certificats autosignés.
- 11 Cliquez sur **Tester la connexion**.
- 12 Cliquez sur **Ajouter**.

Remplacer un serveur de messagerie sortant par défaut du système

Si l'administrateur système a configuré un serveur de messagerie sortant par défaut du système, l'administrateur de locataire peut remplacer ce paramètre global.

Prérequis

Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

- 1 Sélectionnez **Administration > Notifications > Serveurs de messagerie**.
- 2 Sélectionnez le serveur de messagerie sortant.
- 3 Cliquez sur **Remplacer les valeurs globales**.
- 4 Entrez un nom dans la zone de texte **Nom**.
- 5 (Facultatif) Entrez une description dans la zone de texte **Description**.
- 6 Saisissez le nom du serveur dans la zone de texte **Nom du serveur**.
- 7 Choisissez une méthode de chiffrement.
 - Cliquez sur **Utiliser SSL**.
 - Cliquez sur **Utiliser TLS**.
 - Cliquez sur **Aucune** pour envoyer des communications non chiffrées.
- 8 Tapez le numéro de port du serveur dans la zone de texte **Port du serveur**.
- 9 (Facultatif) Cochez la case **Requise** si le serveur requiert une authentification.
 - a Tapez un nom d'utilisateur dans la zone de texte **Nom d'utilisateur**.
 - b Tapez un mot de passe dans la zone de texte **Mot de passe**.
- 10 Tapez l'adresse électronique devant s'afficher pour l'expéditeur de vRealize Automation dans la zone de texte **Adresse de l'expéditeur**.

Cette adresse électronique correspond au nom d'utilisateur et au mot de passe que vous avez fournis.
- 11 Choisissez si vRealize Automation peut accepter des certificats autosignés du serveur de messagerie.

Cette option est disponible uniquement si vous avez activé le chiffrement.

 - Cliquez sur **Oui** pour accepter les certificats autosignés.
 - Cliquez sur **Non** pour rejeter les certificats autosignés.
- 12 Cliquez sur **Tester la connexion**.
- 13 Cliquez sur **Ajouter**.

Remplacer un serveur de messagerie entrant par défaut du système

Si l'administrateur système a configuré un serveur de messagerie entrant par défaut du système, les administrateurs de locataire peuvent remplacer ce paramètre global.

Prérequis

Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

- 1 Sélectionnez **Administration > Notifications > Serveurs de messagerie**.
- 2 Sélectionnez le serveur de messagerie entrant dans la table Serveurs de messagerie.
- 3 Cliquez sur **Remplacer les valeurs globales**.
- 4 Entrez les options de serveur de messagerie entrant suivantes.

Option	Action
Nom	Entrez le nom du serveur de messagerie entrant.
Description	Entrez une description du serveur de messagerie entrant.
Sécurité	Cochez la case SSL pour utiliser SSL pour la sécurité.
Protocole	Choisissez un protocole de serveur.
Nom du serveur	Entrez le nom du serveur.
Port du serveur	Entrez le numéro de port du serveur.

- 5 Tapez le nom du dossier des e-mails dans la zone de texte **Nom de dossier**.
Cette option est requise uniquement si vous choisissez le protocole de serveur IMAP.
- 6 Entrez un nom d'utilisateur dans la zone de texte **Nom d'utilisateur**.
- 7 Entrez un mot de passe dans la zone de texte **Mot de passe**.
- 8 Tapez l'adresse électronique à laquelle les utilisateurs de vRealize Automation peuvent répondre dans la zone de texte **Adresse électronique**.
- 9 (Facultatif) Sélectionnez **Supprimer du serveur** pour supprimer du serveur tous les e-mails traités récupérés par le service de notification.
- 10 Choisissez si vRealize Automation peut accepter des certificats autosignés du serveur de messagerie.
Cette option est disponible uniquement si vous avez activé le chiffrement.
 - Cliquez sur **Oui** pour accepter les certificats autosignés.
 - Cliquez sur **Non** pour rejeter les certificats autosignés.
- 11 Cliquez sur **Tester la connexion**.
- 12 Cliquez sur **Ajouter**.

Rétablir les serveurs de messagerie par défaut du système

Les administrateurs de locataire qui remplacent les serveurs par défaut du système peuvent rétablir les paramètres aux paramètres globaux.

Prérequis

Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

- 1 Sélectionnez **Administration > Notifications > Serveurs de messagerie**.
- 2 Sélectionnez le serveur de messagerie à rétablir.
- 3 Cliquez sur **Rétablir les valeurs globales**.
- 4 Cliquez sur **Oui**.

Configurer des notifications

Chaque utilisateur indique s'il reçoit des notifications, mais les administrateurs de locataire déterminent quels événements déclenchent des notifications.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.
- Vérifiez qu'un administrateur de locataire ou un administrateur système a configuré un serveur de messagerie sortante. Reportez-vous à [Ajouter un serveur de messagerie sortant spécifique à un locataire](#).

Procédure

- 1 Sélectionnez **Administration > Notifications > Scénarios**.
- 2 Sélectionnez une ou plusieurs notifications.
- 3 Cliquez sur **Activer**.

Les utilisateurs abonnés aux notifications dans leurs paramètres de préférence reçoivent maintenant des notifications.

Personnaliser la date de notification par e-mail de l'expiration d'une machine

Vous pouvez spécifier à quel moment une notification par e-mail doit être envoyée avant la date d'expiration d'une machine.

Vous pouvez modifier le paramètre qui définit le nombre de jours avant l'expiration d'une machine avant que vRealize Automation envoie une notification d'expiration par e-mail. L'e-mail avertit les utilisateurs de la date d'expiration d'une machine. Le paramètre par défaut est 7 jours avant l'expiration de la machine.

Procédure

- 1 Connectez-vous au serveur vRealize Automation en utilisant des informations d'identification avec un accès d'administrateur.
- 2 Recherchez et ouvrez le fichier `/etc/vcac/setenv-user`.
- 3 Ajoutez la ligne suivante au fichier pour spécifier le nombre de jours avant la date d'expiration d'une machine, où 3 dans cet exemple spécifie 3 jours avant l'expiration de la machine.

```
VCAC_OPTS="$VCAC_OPTS -Dlease.enforcement.prearchive.notification.days=3"
```

- 4 Redémarrez les services vCAC sur le dispositif virtuel en exécutant la commande suivante :

```
service vcac-server restart
```

Suivant

Si vous travaillez dans un environnement d'équilibrage de charge à haute disponibilité, répétez cette procédure pour tous les dispositifs virtuels dans l'environnement.

Configuration de modèles pour les e-mails IaaS automatiques

Vous pouvez configurer des e-mails de notification à envoyer aux propriétaires de machines concernant plusieurs événements vRealize Automation qui concernent leurs machines.

Les événements qui déclenchent des notifications peuvent inclure l'expiration ou l'expiration imminente des périodes d'archivage et des baux de machines virtuelles.

Pour plus d'informations sur la configuration et l'activation ou la désactivation des notifications par e-mail de vRealize Automation, reportez-vous à l'article de blog et aux articles de la base de connaissances suivants :

- [Personnalisation d'e-mails dans vRealize Automation](#)
- [Personnalisation de modèles d'e-mails dans vRealize Automation \(2088805\)](#)
- [Exemples de personnalisation de modèles d'e-mails dans vRealize Automation \(2102019\)](#)

S'abonner aux notifications

Si vos administrateurs ont configuré des notifications, vous pouvez vous abonner pour recevoir des notifications de vRealize Automation. Les événements de notification peuvent inclure l'exécution réussie d'une demande de catalogue ou d'une approbation requise.

Prérequis

Connectez-vous à la console vRealize Automation.

Procédure

- 1 Cliquez sur **Préférences**.
- 2 Cochez la case **Activé** du protocole de messagerie du tableau Notifications.
- 3 Cliquez sur **Appliquer**.
- 4 Cliquez sur **Fermer**.

(Facultatif) Créer un fichier Remote Desktop Protocol (RDP) personnalisé pour prendre en charge les connexions RDP des machines provisionnées

Les administrateurs système créent un fichier RDP personnalisé que les architectes IaaS utilisent dans les Blueprints afin de configurer les paramètres RDP. Créez le fichier RDP et fournissez aux architectes son nom de chemin complet afin qu'ils puissent l'inclure dans des Blueprints. Un administrateur du catalogue doit ensuite accorder aux utilisateurs un droit d'accès à l'action RDP.

Remarque La configuration de sécurité renforcée d'Internet Explorer ne permet pas de télécharger les fichiers .rdp.

Prérequis

Connectez-vous à IaaS Manager Service en tant qu'administrateur.

Procédure

- 1 Définissez le répertoire actuel sur `<vRA_installation_dir>\Rdp`.
- 2 Copiez le fichier `Default.rdp` et renommez-le `Console.rdp` sans le changer de répertoire.
- 3 Ouvrez le fichier `Console.rdp` dans un éditeur.
- 4 Ajoutez les paramètres RDP au fichier.
Par exemple, **connect to console:i:1**.
- 5 Si vous utilisez un environnement distribué, connectez-vous en tant qu'utilisateur disposant de privilèges administratifs à la machine hôte IaaS sur laquelle le composant Model Manager Website est installé.
- 6 Copiez le fichier `Console.rdp` dans le répertoire `vRA_installation_dir\Website\Rdp`.

Les architectes IaaS peuvent ajouter les propriétés personnalisées RDP aux Blueprints de la machine Windows. Les administrateurs du catalogue peuvent ensuite accorder aux utilisateurs un droit d'accès à l'action Se connecter via RDP. Reportez-vous à [Ajoutez la prise en charge de connexion RDP à vos Blueprints de machine Windows](#).

(Facultatif) Scénario : ajouter des emplacements de centre de données pour des déploiements inter-région

En tant qu'administrateur système, vous souhaitez définir des emplacements pour vos centres de données de Boston et de Londres, afin que les administrateurs Fabric puissent appliquer les emplacements appropriés aux ressources de calcul de chaque centre de données. Lorsque les architectes de Blueprint créent des Blueprints, ils peuvent activer la fonctionnalité des emplacements afin que les utilisateurs puissent choisir de provisionner des machines de Boston ou de Londres lorsqu'ils complètent leurs formulaires de demande d'éléments de catalogue.

Vous voulez éviter que les utilisateurs du centre de données de Boston ne provisionnent des machines de l'infrastructure de Londres, et que les utilisateurs du centre de données de Londres ne provisionnent des machines de l'infrastructure de Boston. Pour vous assurer que les utilisateurs de Boston ne provisionnent que l'infrastructure de Boston, et ceux de Londres celle de Londres uniquement, vous souhaitez autoriser les utilisateurs à sélectionner l'emplacement de provisionnement adéquat lors de leur demande de machines.



Vous ne pouvez pas filtrer les emplacements de centre de données dans le fichier xml basé sur le locataire ou le groupe d'activité. Lorsque vous travaillez dans un environnement à locataires multiples, vous pouvez utiliser des définitions de propriétés pour filtrer en fonction du locataire ou du groupe d'activité. Pour plus d'informations sur l'utilisation de définitions de propriétés, reportez-vous au billet de blog [Utilisation des définitions de propriétés dynamiques](#).

Procédure

- 1 Connectez-vous à l'hôte du serveur Web IaaS à l'aide des informations d'identification de l'administrateur.
Il s'agit de la machine sur laquelle vous avez installé le composant du site Web IaaS.
- 2 Modifiez le fichier `WebSite\XmlData\DataCenterLocations.xml` dans l'annuaire d'installation du serveur Windows (généralement `%SystemDrive%\Program Files x86\VMware\vCAC\Server`).
- 3 Modifiez la section `CustomDataType` du fichier pour créer les entrées Nom des données de chaque emplacement.

```
<CustomDataType>
  <Data Name="London" Description="London datacenter" />
  <Data Name="Boston" Description="Boston datacenter" />
</CustomDataType>
```

- 4 Enregistrez et fermez le fichier.
- 5 Redémarrez Manager Service.
- 6 Si vous possédez plusieurs hôtes du serveur Web IaaS, répétez cette procédure sur chaque instance redondante.

L'administrateur Fabric peut appliquer l'emplacement approprié aux ressources de calcul de chaque centre de données. Reportez-vous à [Scénario : appliquer un emplacement à une ressource de calcul pour des déploiements inter-région](#).

Suivant

Vous pouvez ajouter la propriété `Vrm.DataCenter.Location` à un Blueprint ou activer l'option **Afficher l'emplacement à la demande** dans le Blueprint, pour demander à l'utilisateur de spécifier un emplacement de centre de données lorsqu'il demande le provisionnement d'une machine.

Configuration de vRealize Orchestrator

vRealize Orchestrator est un moteur d'automatisation et de gestion qui étend vRealize Automation afin de prendre en charge XaaS et d'autres extensibilités. Vous pouvez configurer et utiliser le serveur vRealize Orchestrator qui est préconfiguré dans le dispositif vRealize Automation, ou vous pouvez déployer vRealize Orchestrator comme une instance de serveur externe et associer cette instance externe à vRealize Automation.

vRealize Orchestrator permet aux administrateurs et aux architectes de développer des tâches d'automatisation complexes à l'aide du concepteur de workflow, puis d'accéder aux workflows et de les exécuter à partir de vRealize Automation.

vRealize Orchestrator peut accéder aux technologies et aux applications externes, et les contrôler, à l'aide des plug-ins vRealize Orchestrator.

La configuration de vRealize Automation pour utiliser vRealize Orchestrator permet de publier des workflows Orchestrator dans le catalogue de services vRealize Orchestrator dans le cadre de la gestion de blueprints XaaS.

Si vous souhaitez exécuter des workflows Orchestrator pour étendre la gestion des machines IaaS, vous devez configurer vRealize Orchestrator comme un point de terminaison.

Privilèges de configuration

Les administrateurs système et les administrateurs de locataire peuvent configurer vRealize Automation pour utiliser un serveur externe ou le serveur vRealize Orchestrator intégré.

De plus, les administrateurs système peuvent déterminer les dossiers de workflow mis à disposition de chaque locataire.

Les administrateurs de locataire peuvent configurer les plug-ins vRealize Orchestrator en tant que points de terminaison.

Rôle	Privilèges de configuration liés à vRealize Orchestrator
Administrateurs système	<ul style="list-style-type: none"> ■ Configurer le serveur vRealize Orchestrator pour tous les locataires ■ Définir les dossiers de workflow vRealize Orchestrator par défaut par locataire
Administrateurs de locataire	<ul style="list-style-type: none"> ■ Configurer le serveur vRealize Orchestrator pour leur propre locataire ■ Ajouter les plug-ins vRealize Orchestrator en tant que points de terminaison

Configurer le serveur vRealize Orchestrator intégré

Le dispositif vRealize Automation inclut une instance préconfigurée de vRealize Orchestrator. Le service du serveur vRealize Orchestrator est en cours d'exécution par défaut, mais vous devez démarrer le service de configuration manuellement pour accéder au centre de contrôle.

Prérequis

Déployez le dispositif vRealize Automation. Pour plus d'informations, reportez-vous à la section *Déployer le dispositif vRealize Automation* dans *Installation de vRealize Automation 7.3*.

Procédure

- 1 Connectez-vous à la console vRealize Automation en tant qu'**administrateur système** ou **administrateur de locataire**.
- 2 Sélectionnez **Administration > Configuration vRO > Configuration du serveur**.
- 3 Cliquez sur **Utilisez le serveur Orchestrator par défaut**.

Les connexions au serveur vRealize Orchestrator intégré sont maintenant configurées. Le dossier de workflows **VCAC** et les actions de l'utilitaire associées sont importées automatiquement. Le dossier de workflows **VCAC > ASD** contient les workflows de configuration des points de terminaison et de création du mappages de ressources.

Configurer le dossier de workflow par défaut d'un locataire

Les administrateurs système peuvent regrouper des workflows dans différents dossiers, puis définir des catégories de workflow par locataire. Ce faisant, ils peuvent autoriser des utilisateurs de différents locataires à accéder à plusieurs dossiers de workflow sur le même serveur vRealize Orchestrator.

Prérequis

Connectez-vous à la console de vRealize Automation en tant qu'**administrateur système**.

Procédure

- 1 Sélectionnez **Administration > Services avancés > Dossier vRO par défaut**.
- 2 Cliquez sur le nom du locataire que vous souhaitez modifier.
- 3 Parcourez la bibliothèque de workflows vRealize Orchestrator et sélectionnez un dossier.
- 4 Cliquez sur **Ajouter**.

Vous avez défini le dossier de workflow vRealize Orchestrator d'un locataire par défaut.

Suivant

Répétez la procédure pour tous les locataires pour lesquels vous souhaitez définir un dossier de workflow par défaut.

Se connecter à l'interface de configuration de vRealize Orchestrator

Pour modifier la configuration de l'instance de vRealize Orchestrator par défaut intégrée à vRealize Automation, démarrez le service de configuration de vRealize Orchestrator et connectez-vous à l'interface de configuration de vRealize Orchestrator.

Le service de configuration de vRealize Orchestrator ne démarre pas par défaut dans le dispositif vRealize Automation. Vous devez démarrer le service de configuration de vRealize Orchestrator pour accéder à l'interface de configuration de vRealize Orchestrator.

Procédure

- 1 Démarrez le service de configuration de vRealize Orchestrator.
 - a Connectez-vous à la console Linux du dispositif vRealize Automation en tant qu'utilisateur racine.
 - b Entrez **service vco-configurator start** et appuyez sur Entrée.

- 2 Se connecter à l'URL vRealize Automation dans un navigateur Web.

- 3 Cliquez sur **Centre de contrôle vRealize Orchestrator**.

Vous êtes redirigé vers https://vra-va-hostname.domain.name_or_load_balancer_address:8283/vco-controlcenter.

- 4 Connectez-vous au centre de contrôle vRealize Orchestrator.

Le nom d'utilisateur est configuré par l'administrateur du dispositif vRealize Automation.

Connectez-vous au client vRealize Orchestrator .

Pour effectuer des tâches d'administration générale ou pour modifier ou créer des workflows dans l'instance de vRealize Orchestrator par défaut, vous devez vous connecter au client vRealize Orchestrator.

L'interface du client vRealize Orchestrator est conçue pour les développeurs disposant de droits administratifs souhaitant développer des workflows, des actions et d'autres éléments personnalisés.

Procédure

- 1 Connectez-vous à l'URL de vRealize Automation dans un navigateur Web.

- 2 Cliquez sur **vRealize Orchestrator Client**.

Le fichier client est téléchargé.

- 3 Cliquez sur le téléchargement et suivez les invites qui s'affichent.

- 4 Sur la page de connexion à vRealize Orchestrator, entrez l'IP ou le nom de domaine du dispositif vRealize Automation dans la zone de texte **Nom d'hôte** et **443** comme numéro de port par défaut.

Par exemple, entrez *vrealize_automation_appliance_ip:443*.

- 5 Connectez-vous à l'aide du nom d'utilisateur et du mot de passe du client vRealize Orchestrator.

Les informations d'identification correspondent au nom d'utilisateur et au mot de passe de l'administrateur de locataire par défaut.

- 6 Dans la fenêtre **Avertissement de certificat**, sélectionnez une option pour gérer l'avertissement de certificat.

vRealize Orchestrator Client communique avec le serveur vRealize Orchestrator à l'aide d'un certificat SSL. Une autorité de certification approuvée ne signe pas le certificat pendant l'installation. Vous recevez un avertissement de certificat à chaque fois que vous vous connectez au serveur vRealize Orchestrator.

Option	Description
Ignorer	Continuez avec le certificat SSL actuel. Le message d'avertissement s'affichera à nouveau lorsque vous vous reconnecterez au même serveur vRealize Orchestrator ou lorsque vous essaierez de synchroniser un workflow avec un serveur vRealize Orchestrator distant.
Annuler	Fermez la fenêtre et arrêtez le processus de connexion.
Installer ce certificat et ne plus afficher aucun avertissement de sécurité pour ce serveur.	Cochez cette case et cliquez sur Ignorer pour installer le certificat et ne plus recevoir les avertissements de sécurité.

Vous pouvez remplacer le certificat SSL par défaut par un certificat signé par une autorité de certification. Pour plus d'informations sur la modification des certificats SSL, reportez-vous à la section *Installation et configuration de VMware vRealize Orchestrator*.

Suivant

Vous pouvez importer un package, développer des workflows ou définir des droits d'accès root sur le système. Reportez-vous à *Utilisation de VMware vRealize Orchestrator Client et Développement avec VMware vRealize Orchestrator*.

Configurer un serveur vRealize Orchestrator externe

Vous pouvez configurer vRealize Automation afin d'utiliser un serveur vRealize Orchestrator externe.

Les administrateurs système peuvent configurer globalement le serveur vRealize Orchestrator par défaut pour tous les locataires. Les administrateurs de locataire peuvent configurer le serveur vRealize Orchestrator uniquement pour leurs locataires.

Les connexions aux instances du serveur vRealize Orchestrator externe impliquent l'octroi au compte d'utilisateur des autorisations d'affichage et d'exécution dans vRealize Orchestrator.

- **Authentification Single Sign-On.** Les informations utilisateur sont transmises à vRealize Orchestrator avec la demande XaaS et l'utilisateur reçoit les autorisations d'affichage et d'exécution pour le workflow demandé.
- **Authentification de base.** Le compte d'utilisateur fourni doit être membre d'un groupe vRealize Orchestrator disposant des autorisations d'affichage et d'exécution, ou membre du groupe vcoadmins.

Prérequis

- Installez et configurez un dispositif vRealize Orchestrator externe. Reportez-vous à la section *Installation et configuration de vRealize Orchestrator* dans le Centre d'informations de vRealize Orchestrator sur https://www.vmware.com/support/pubs/orchestrator_pubs.html.
- Connectez-vous à la console vRealize Automation en tant qu'**administrateur système** ou **administrateur de locataire**.
- Configurez le dossier de workflows par défaut. Reportez-vous à [Configurer le dossier de workflow par défaut d'un locataire](#).

Procédure

- 1 Sélectionnez **Administration > Configuration vRO > Configuration du serveur**.
- 2 Cliquez sur **Utilisez un serveur Orchestrator externe**.
- 3 Entrez un nom et, éventuellement, une description.
- 4 Dans la zone de texte **Hôte**, entrez l'adresse IP ou le nom DNS de la machine sur laquelle le serveur vRealize Orchestrator est exécuté.

Remarque Si l'instance externe d'Orchestrator est configurée pour fonctionner en mode cluster, entrez l'adresse IP ou le nom d'hôte du serveur virtuel d'équilibrage de charge qui distribue les demandes des clients sur les serveurs Orchestrator dans le cluster.

- 5 Dans la zone de texte **Port**, entrez le numéro de port pour communiquer avec le serveur vRealize Orchestrator externe.

Le port par défaut de vRealize Orchestrator est 8281.

- 6 Sélectionnez le type d'authentification.

Option	Description
Single Sign-On	Établit une connexion avec le serveur vRealize Orchestrator à l'aide de vCenter Single Sign-On. Cette option s'applique uniquement si vous avez configuré vRealize Orchestrator et vRealize Automation pour utiliser une instance commune de vCenter Single Sign-On.
De base	Établit une connexion avec le serveur vRealize Orchestrator à l'aide du nom d'utilisateur et du mot de passe que vous avez entrés dans les zones de texte Nom d'utilisateur et Mot de passe . Le compte fourni doit être membre du groupe vcoadmins vRealize Orchestrator ou membre d'un groupe qui dispose des autorisations d'affichage et d'exécution.

- 7 Cliquez sur **Tester la connexion**.
- 8 Cliquez sur **OK**.

Vous avez configuré la connexion au serveur vRealize Orchestrator externe. Le dossier de workflows **vCAC** et les actions de l'utilitaire associé sont automatiquement importées. Le dossier de workflows **vCAC > ASD** contient les workflows de configuration des points de terminaison et de création du mappages de ressources.

Suivant

[Connectez-vous au client vRealize Orchestrator.](#)

Configuration des ressources

Vous pouvez configurer des ressources, telles que des points de terminaison, des réservations et des profils réseau pour prendre en charge la définition de Blueprints vRealize Automation et le provisionnement de machines.

Liste de contrôle pour la configuration de ressources IaaS

Les administrateurs IaaS et les administrateurs Fabric configurent les ressources IaaS pour intégrer l'infrastructure existante à vRealize Automation et pour allouer des ressources d'infrastructure à des groupes d'activité vRealize Automation.

Vous pouvez utiliser la liste de contrôle Configuration des ressources IaaS pour voir un aperçu de haut niveau de la séquence d'étapes requises pour configurer des ressources IaaS.

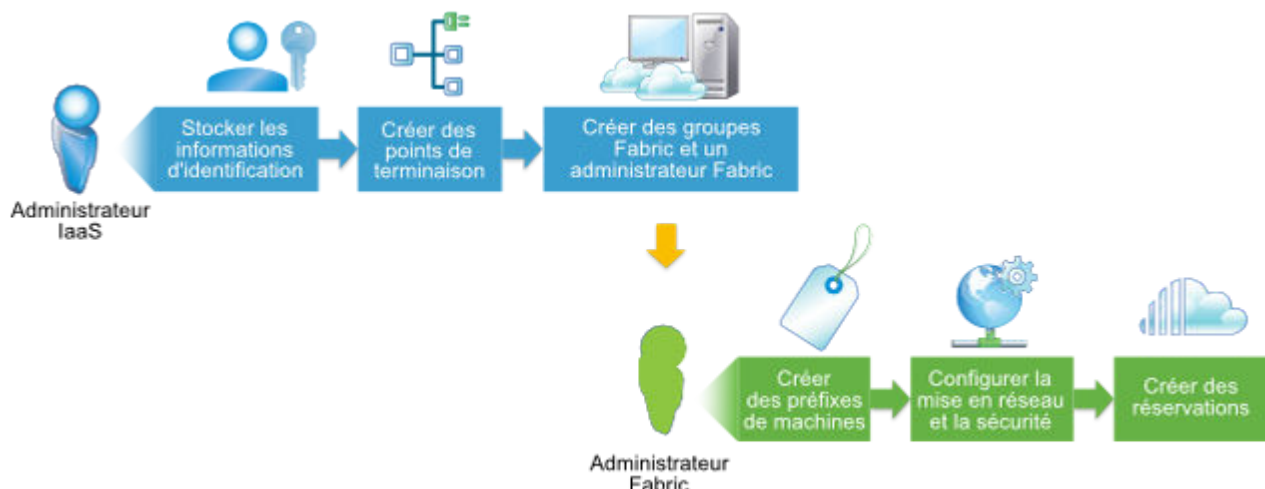


Tableau 2-11. Liste de contrôle pour la configuration de ressources IaaS

Tâche	Rôle vRealize Automation	Détails
<input type="checkbox"/> Créer des points de terminaison pour votre infrastructure afin de mettre les ressources sous la gestion de vRealize Automation.	Administrateur IaaS	Choisir un scénario de point de terminaison.
<input type="checkbox"/> Créer un groupe Fabric pour organiser les ressources d'infrastructure en groupes et affecter un ou plusieurs administrateurs pour gérer ses ressources en tant qu'administrateurs Fabric de vRealize Automation.	Administrateur IaaS	Créer un groupe Fabric.
<input type="checkbox"/> Configurer des préfixes de machine servant à créer des noms pour les machines provisionnées via vRealize Automation.	Administrateur Fabric	Configurer des préfixes de machines.
<input type="checkbox"/> (Facultatif) Créer des profils réseau pour configurer des paramètres réseau pour les machines provisionnées.	Administrateur Fabric	Création d'un profil réseau.
<input type="checkbox"/> Allouer des ressources d'infrastructure à des groupes d'activité en créant des réservations et, facultativement, des profils de réservation et de réservation de stockage.	<ul style="list-style-type: none"> ■ Administrateur IaaS s'il est également configuré comme administrateur Fabric ■ Administrateur Fabric 	Configuration de réservations et de stratégies de réservation.

Configuration de points de terminaison

Vous créez et configurez les points de terminaison qui permettent à vRealize Automation de communiquer avec votre infrastructure.

Les définitions de points de terminaison sont classées en fonction du type :

- Cloud

La catégorie de cloud contient les types de point de terminaison vCloud Air, vCloud Director, Amazon EC2 et OpenStack

- IPAM

Cette catégorie est uniquement visible si vous avez enregistré un type de point de terminaison IPAM tiers tel qu'Infoblox IPAM dans un workflow vRealize Orchestrator.

- Gestion

Cette catégorie contient le point de terminaison vRealize Operations Manager uniquement.

- Réseau et sécurité

Cette catégorie contient les types de point de terminaison proxy et NSX.

Un point de terminaison proxy peut être associé à un point de terminaison Amazon, vCloud Air ou vCloud Director.

Un point de terminaison NSX peut être associé à un point de terminaison vSphere.

- Orchestration

Cette catégorie contient le point de terminaison vRealize Orchestrator uniquement.

- Stockage

Cette catégorie contient le point de terminaison NetApp ONTAP.

- Virtuel

La catégorie virtuelle contient les types de point de terminaison vSphere, Hyper-V (SCVMM) et KVM (RHEV).

Vous pouvez configurer des types de point de terminaison supplémentaires dans vRealize Orchestrator et les utiliser avec des types de point de terminaison pris en charge dans vRealize Automation. Vous pouvez également importer et exporter des points de terminaison par programmation.

Pour plus d'informations sur l'utilisation de points de terminaison après la mise à niveau ou la migration, reportez-vous à la section [Éléments à prendre en compte lors de l'utilisation de points de terminaison mis à niveau ou migrés](#).

Choisir un scénario de point de terminaison

Choisissez un scénario de point de terminaison basé sur le type de point de terminaison cible.

Pour plus d'informations sur les paramètres de point de terminaison disponibles, reportez-vous à la section [Référence des paramètres de point de terminaison](#).

Tableau 2-12. Choisir un scénario de point de terminaison

Point de terminaison	Plus d'informations
vSphere	Créer un point de terminaison vSphere
NSX	Créer un point de terminaison NSX et l'associer à un point de terminaison vSphere
vCloud Air sur abonnement ou à la demande	Créer un point de terminaison vCloud Air.
vCloud Director	Créer un point de terminaison vCloud Director.
vRealize Orchestrator	Créer un point de terminaison vRealize Orchestrator.
vRealize Operations	Créer un point de terminaison vRealize Operations Manager
Fournisseur IPAM tiers	Créer un point de terminaison de fournisseur IPAM tiers
Microsoft Azure	Créer un point de terminaison Microsoft Azure
Puppet	Créer un point de terminaison Puppet
Amazon	<ul style="list-style-type: none"> ■ Créer un point de terminaison Amazon ■ (facultatif) Ajouter un type d'instance Amazon
OpenStack	Créer un point de terminaison OpenStack

Tableau 2-12. Choisir un scénario de point de terminaison (suite)

Point de terminaison	Plus d'informations
Proxy	Créer un point de terminaison proxy et l'associer à un point de terminaison cloud
Hyper-V (SCVMM)	Créer un point de terminaison Hyper-V (SCVMM)
KVM (RHEV)	Référence des paramètres de point de terminaison
NetApp ONTAP	<ul style="list-style-type: none"> ■ Stockage à optimisation d'espace pour le provisionnement virtuel ■ Référence des paramètres de point de terminaison
Hyper-V (autonome), XenServer ou serveur maître du pool Xen	Créer un point de terminaison Hyper-V, XenServer ou de pool Xen
Importer des points de terminaison	Importer ou exporter des points de terminaison par programme

Référence des paramètres de point de terminaison

Utilisez les paramètres de point de terminaison pour définir l'emplacement et accéder aux informations d'identification pour la collecte des données et le déploiement du catalogue de services.

Onglet Général

La plupart des points de terminaison vRealize Automation contiennent les options suivantes. Les paramètres propres à un type de point de terminaison spécifique sont signalés.

Tableau 2-13. Paramètres de l'onglet Général

Configuration	Description
Nom	Entrez le nom du point de terminaison.
Description	Entrez la description du point de terminaison.

Tableau 2-13. Paramètres de l'onglet **Général** (suite)

Configuration	Description
Adresse	<p>Entrez l'adresse du point de terminaison en utilisant le format d'adresse spécifique au point de terminaison.</p> <ul style="list-style-type: none"> Pour un point de terminaison KVM (RHEV) ou NetApp ONTAP, l'adresse doit être dans l'un des formats suivants : <ul style="list-style-type: none"> <code>https://FQDN</code> <code>https://IP_address</code> <p>Par exemple : <code>https://mycompany-kvmrhev1.mycompany.local</code> ou <code>netapp-1.mycompany.local</code>.</p> Pour un point de terminaison OpenStack, l'adresse doit être au format <code>https:// FQDN/powervc/openstack/ service</code>. Par exemple : <code>https://openstack.mycompany.com/powervc/openstack/admin</code>. Pour un point de terminaison OpenStack, l'adresse doit être dans l'un des formats suivants : <ul style="list-style-type: none"> <code>https://FQDN:500</code> <code>https://IP_address:500</code> Pour un point de terminaison vSphere, l'adresse doit être au format <code>https:// host/sdk</code>. Pour un point de terminaison NSX, l'adresse doit être au format <code>https://host</code>. Pour un point de terminaison vRealize Orchestrator, l'adresse doit être dans le protocole HTTPS et inclure le nom complet ou l'adresse IP du serveur vRealize Orchestrator et le numéro de port vRealize Orchestrator, par exemple <code>https://vrealize-automation-appliance-hostname:443/vco</code>. Pour un point de terminaison vRealize Operations, l'adresse doit être au format <code>https:// host/suite-api</code>.
Informations d'identification intégrées	<p>Si vous choisissez d'utiliser vos informations d'identification vSphere intégrées, il est inutile d'entrer un nom d'utilisateur et le mot de passe.</p> <p>Ce paramètre s'applique uniquement aux points de terminaison vSphere.</p>
Nom d'utilisateur	Entrez le nom d'utilisateur de niveau administrateur que vous avez stocké pour le point de terminaison dans le format spécifique aux points de terminaison, comme indiqué dans l'interface utilisateur.
Mot de passe	Entrez le mot de passe de niveau administrateur que vous avez stocké pour le point de terminaison.
Projet OpenStack	<p>Entrez un nom de locataire OpenStack.</p> <p>Ce paramètre s'applique uniquement aux points de terminaison OpenStack.</p>
Organisation	<p>Si vous êtes l'administrateur d'une organisation, vous pouvez entrer le nom d'une organisation vCloud Director.</p> <p>Ce paramètre s'applique uniquement à vCloud Director.</p>
ID de clé d'accès	<p>Entrez l'ID de clé Amazon AWS.</p> <p>Ce paramètre s'applique uniquement aux points de terminaison Amazon.</p>
Clé d'accès secrète	<p>Entrez votre clé d'accès secrète Amazon AWS.</p> <p>Ce paramètre s'applique uniquement aux points de terminaison Amazon.</p>

Tableau 2-13. Paramètres de l'onglet Général (suite)

Configuration	Description
Port	Entrez la valeur du port auquel se connecter sur l'adresse du point de terminaison proxy. Ce paramètre s'applique uniquement aux points de terminaison Proxy.
Priorité	Entrez comme valeur de priorité un nombre entier supérieur ou égal à 1. La valeur inférieure spécifie une priorité plus élevée. La valeur de priorité est associée à la propriété personnalisée VMware.VCenterOrchestrator.Priority intégrée. Ce paramètre s'applique uniquement aux points de terminaison vRealize Orchestrator.

Onglet Propriétés

Tous les types de point de terminaison utilisent un onglet Propriétés pour capturer des propriétés personnalisées ou des groupes de propriétés et des paramètres. Pour consulter des exemples de propriétés personnalisées pour des types de point de terminaison spécifiques, reportez-vous à la section *Référence des propriétés personnalisées*.

Onglet Association

Vous pouvez créer une association à un point de terminaison NSX ou un point de terminaison Proxy, selon le point de terminaison à partir duquel vous créez l'association. Vous pouvez associer un point de terminaison vSphere avec un point de terminaison NSX pour affecter des paramètres de NSX au point de terminaison vSphere. Vous pouvez également associer un point de terminaison vCloud Air, vCloud Director ou Amazon à un point de terminaison proxy pour affecter des paramètres de proxy au point de terminaison vCloud Air, vCloud Director ou Amazon.

Tester la connexion

Vous pouvez utiliser une action de test des connexions pour valider les informations d'identification, l'adresse du point de terminaison hôte et le certificat d'un point de terminaison vSphere, NSX ou vRealize Operations Manager. Reportez-vous à [Considérations sur l'utilisation du test des connexions](#).

Créer un point de terminaison vSphere

Vous pouvez créer des points de terminaison permettant à vRealize Automation de communiquer avec l'environnement vSphere et découvrir les ressources de calcul, collecter les données et provisionner les machines. Vous pouvez également associer des paramètres NSX au point de terminaison vSphere en associant ce dernier à un point de terminaison NSX.

Si vous avez mis à niveau ou migré un point de terminaison vSphere qui utilisait un gestionnaire NSX, un nouveau point de terminaison NSX est créé, qui contient une association entre le point de terminaison vSphere source et un nouveau point de terminaison NSX.

Si votre environnement vSphere est intégré à NSX, reportez-vous à [Créer un point de terminaison NSX et l'associer à un point de terminaison vSphere](#).

Pour en savoir plus sur la validation de la connexion et l'approbation de certificat, reportez-vous à la section [Considérations sur l'utilisation du test des connexions](#).

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur laaS**.
- Vous devez installer un agent proxy vSphere pour gérer votre point de terminaison vSphere et vous devez utiliser exactement le même nom pour l'agent et le point de terminaison. Pour plus d'informations sur l'installation de l'agent, reportez-vous à *Installation de vRealize Automation 7.3*.
- Si vous souhaitez configurer les paramètres de réseau et de sécurité NSX supplémentaires pour le point de terminaison vSphere, créez un point de terminaison NSX. Vous pouvez effectuer une association au point de terminaison NSX lorsque vous créez le point de terminaison vSphere. Reportez-vous à [Créer un point de terminaison NSX et l'associer à un point de terminaison vSphere](#).

Procédure

- 1 Sélectionnez **Infrastructure > Points de terminaison > Points de terminaison**.

- 2 Sélectionnez **Nouveau > Virtuel > vSphere**.

- 3 Entrez un nom dans la zone de texte **Nom**.

Le nom doit correspondre au nom du point de terminaison fourni à l'agent proxy vSphere lors de l'installation, sinon la collecte des données échoue.

- 4 (Facultatif) Entrez une description dans la zone de texte **Description**.

- 5 Entrez l'URL de l'instance vCenter Server dans la zone de texte **Adresse**.

L'URL doit être du type : **https://nom_d'hôte/sdk** ou **https://adresse_IP/sdk**.

Par exemple, **https://vsphereA/sdk**.

- 6 Entrez votre nom d'utilisateur de niveau administrateur et votre mot de passe vSphere ou utilisez vos informations d'identification intégrées vSphere.

Fournissez des informations d'identification dotées de l'autorisation de modifier des attributs personnalisés.

Le format du nom d'utilisateur est *domain\username*.

Sélectionnez **Utiliser les informations d'identification intégrées** afin d'utiliser le compte de service de l'agent proxy vSphere pour vous connecter à vCenter Server.

Si vous choisissez d'utiliser vos informations d'identification vSphere intégrées, il est inutile d'entrer un nom d'utilisateur et le mot de passe.

- 7 (Facultatif) Cliquez sur **Propriétés** et ajoutez des propriétés personnalisées fournies, des groupes de propriétés ou vos propres définitions de propriétés pour le point de terminaison.
- 8 (Facultatif) Pour configurer les paramètres de réseau et de sécurité NSX pour le point de terminaison, cliquez sur **Associations** et établissez une association à un point de terminaison NSX existant.

Vous devez disposer d'au moins un point de terminaison NSX pour créer une association.

- 9 (Facultatif) Cliquez sur **Tester la connexion** pour valider les informations d'identification, l'adresse de point de terminaison d'hôte et le certificat de confiance. L'action vérifie également que Service Manager et l'agent sont en cours d'exécution afin que le point de terminaison puisse faire l'objet d'une collecte de données. L'action **OK** teste ces mêmes conditions.

L'action de **Tester la connexion** renvoie des informations sur une des conditions suivantes :

- Erreur de certificat

Si le certificat n'est pas trouvé, n'est pas approuvé ou a expiré, vous êtes invité à accepter une empreinte numérique de certificat. Si vous n'acceptez pas l'empreinte numérique, vous pouvez toujours enregistrer le point de terminaison, mais le provisionnement de la machine peut échouer.

- Erreur de l'agent

L'agent vSphere associé est introuvable. L'agent doit être en cours d'exécution pour que le test réussisse.

- Erreur de l'hôte

L'adresse de point de terminaison spécifiée n'est pas accessible ou l'instance associée de Manager Service n'est pas en cours d'exécution. Manager Service doit être en cours d'exécution pour que le test réussisse.

- Erreur d'informations d'identification

La combinaison du nom d'utilisateur et du mot de passe spécifiée n'est pas valide pour le point de terminaison à l'adresse spécifiée.

- Délai d'expiration

L'action de test n'a pas pu aboutir dans le délai imparti de deux minutes.

Si l'action **Tester la connexion** échoue, vous pouvez toujours enregistrer le point de terminaison, mais le provisionnement de la machine risque d'échouer.

S'il y a un problème de certificat approuvé, par exemple le certificat a expiré, un message vous invite à accepter une empreinte de certificat.

- 10 Cliquez sur **OK** pour enregistrer le point de terminaison.

L'action **OK** teste les mêmes conditions que l'action de **Tester la connexion**. Si elle trouve l'une des conditions précédentes, elle renvoie un message. Si l'action peut enregistrer, l'erreur reste affichée à l'écran pour vous permettre de la consulter.

vRealize Automation collecte les données de votre point de terminaison et détecte vos ressources de calcul.

Remarque Pour éviter l'échec du provisionnement, ne renommez pas les centres de données vSphere après la collecte des données initiale.

Suivant

Ajoutez des ressources de calcul à partir de votre point de terminaison dans un groupe Fabric. Reportez-vous à [Créer un groupe Fabric](#).

Créer un point de terminaison NSX et l'associer à un point de terminaison vSphere

Vous pouvez créer un point de terminaison NSX et associer ses paramètres NSX à un point de terminaison vSphere existant.

Si vous avez mis à niveau ou migré un point de terminaison vSphere qui utilisait un gestionnaire NSX, un nouveau point de terminaison NSX est créé, qui contient une association entre le point de terminaison vSphere source et un nouveau point de terminaison NSX.

Pour plus d'informations sur la validation de la connexion NSX et l'approbation du certificat, reportez-vous à la section [Considérations sur l'utilisation du test des connexions](#).

Pour plus d'informations sur la création d'un point de terminaison NSX, consultez les articles publics tels que ce [billet du blog vmwarelab](#).

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur laaS**.
- Vous devez installer un agent proxy vSphere pour gérer votre point de terminaison vSphere et vous devez utiliser exactement le même nom pour l'agent et le point de terminaison. Pour plus d'informations sur l'installation de l'agent, reportez-vous à *Installation de vRealize Automation 7.3*.
- Configurez vos paramètres réseau NSX. Reportez-vous à [Configuration des paramètres de composants de réseau et de sécurité](#).
- [Créer un point de terminaison vSphere](#).

En préparation de l'utilisation des capacités de réseau, de sécurité et d'équilibrage de charge NSX dans vRealize Automation, lors de l'utilisation des informations d'identification du gestionnaire NSX vous devez utiliser le compte d'administrateur gestionnaire NSX.

Procédure

- 1 Sélectionnez **Infrastructure > Points de terminaison > Points de terminaison**.
- 2 Sélectionnez **Nouveau > Réseau et sécurité > NSX**.
- 3 Entrez un nom dans la zone de texte **Nom**.
- 4 (Facultatif) Entrez une description dans la zone de texte **Description**.
- 5 Entrez l'URL de l'instance NSX dans la zone de texte **Adresse**.

L'URL doit être du type : **https://nom_d'hôte** ou **https://adresse_IP**.

Par exemple, **https://nsx-manager.local**.

- 6 Entrez le nom d'utilisateur et le mot de passe NSX de niveau administrateur qui sont stockés pour le point de terminaison NSX.

- 7 (Facultatif) Cliquez sur **Propriétés** et ajoutez des propriétés personnalisées fournies, des groupes de propriétés ou vos propres définitions de propriétés pour le point de terminaison.

- 8 Pour associer les paramètres de réseau et de sécurité NSX à un point de terminaison vSphere existant, cliquez sur **Associations** et sélectionnez un point de terminaison vSphere existant.

Vous devez créer le point de terminaison vSphere avant de pouvoir créer l'association.

Vous pouvez uniquement associer un point terminaison NSX à un point de terminaison vSphere.

Cette contrainte d'association signifie que vous ne pouvez pas provisionner un réseau à la demande universel et l'attacher aux machines vSphere provisionnées sur différents serveurs vCenter.

- 9 (Facultatif) Cliquez sur **Tester la connexion** pour valider les informations d'identification, l'adresse de point de terminaison d'hôte et le certificat de confiance. L'action vérifie également que Service Manager et l'agent sont en cours d'exécution afin que le point de terminaison puisse faire l'objet d'une collecte de données. L'action **OK** teste ces mêmes conditions.

L'action de **Tester la connexion** renvoie des informations sur une des conditions suivantes :

- Erreur de certificat

Si le certificat n'est pas trouvé, n'est pas approuvé ou a expiré, vous êtes invité à accepter une empreinte numérique de certificat. Si vous n'acceptez pas l'empreinte numérique, vous pouvez toujours enregistrer le point de terminaison, mais le provisionnement de la machine peut échouer.

- Erreur de l'agent

L'agent vSphere associé est introuvable. L'agent doit être en cours d'exécution pour que le test réussisse.

- Erreur de l'hôte

L'adresse de point de terminaison spécifiée n'est pas accessible ou l'instance associée de Manager Service n'est pas en cours d'exécution. Manager Service doit être en cours d'exécution pour que le test réussisse.

- Erreur d'informations d'identification

La combinaison du nom d'utilisateur et du mot de passe spécifiée n'est pas valide pour le point de terminaison à l'adresse spécifiée.

- Délai d'expiration

L'action de test n'a pas pu aboutir dans le délai imparti de deux minutes.

Si l'action **Tester la connexion** échoue, vous pouvez toujours enregistrer le point de terminaison, mais le provisionnement de la machine risque d'échouer.

S'il y a un problème de certificat approuvé, par exemple le certificat a expiré, un message vous invite à accepter une empreinte de certificat.

- 10 Cliquez sur **OK** pour enregistrer le point de terminaison.

L'action **OK** teste les mêmes conditions que l'action de **Tester la connexion**. Si elle trouve l'une des conditions précédentes, elle renvoie un message. Si l'action peut enregistrer, l'erreur reste affichée à l'écran pour vous permettre de la consulter.

vRealize Automation collecte les données de votre point de terminaison et détecte vos ressources de calcul.

Suivant

Ajoutez des ressources de calcul à partir de votre point de terminaison dans un groupe Fabric. Reportez-vous à [Créer un groupe Fabric](#).

Créez un point de terminaison vCloud Air .

Vous pouvez créer un point de terminaison vCloud Air pour un service à la demande ou sur abonnement. Vous pouvez éventuellement associer les paramètres de proxy au point de terminaison vCloud Director par association à un point de terminaison proxy.

Pour obtenir des informations sur la console de gestion de vCloud Air, reportez-vous à la documentation de vCloud Air.

Remarque Les réservations définies pour les points de terminaison vCloud Air et vCloud Director ne prennent pas en charge l'utilisation de profils réseau pour le provisionnement des machines.

Pour les points de terminaison vCloud Air, le nom de l'organisation et le nom du vDC doivent être identiques pour une instance d'abonnement vCloud Air.

Pour plus d'informations sur l'association des paramètres de proxy à votre point de terminaison, reportez-vous à la section [Créer un point de terminaison proxy et l'associer à un point de terminaison cloud](#).

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur IaaS**.
- Vérifiez que vous disposez d'une autorisation **Administrateur d'infrastructure virtuelle** pour votre service d'abonnement ou votre compte à la demande vCloud Air.
- Si vous souhaitez configurer une sécurité supplémentaire et forcer les connexions à transiter par un serveur proxy, créez un point de terminaison proxy. Vous pouvez associer au point de terminaison proxy lors de la création du point de terminaison vCloud Director. Reportez-vous à [Créer un point de terminaison proxy et l'associer à un point de terminaison cloud](#).

Procédure

- 1 Sélectionnez **Infrastructure > Points de terminaison > Points de terminaison**.
- 2 Sélectionnez **Nouveau > Cloud > vCloud Air**.
- 3 Entrez un nom et, éventuellement, une description.
- 4 Acceptez l'adresse par défaut du point de terminaison vCloud Air dans la zone de texte **Adresse** ou entrez une nouvelle adresse.

L'adresse par défaut du point de terminaison vCloud Air est `https://vca.vmware.com`, spécifiée dans la propriété globale `Default URL for vCloud Air endpoint`.

5 Entrez votre nom d'utilisateur de niveau administrateur et votre mot de passe.

Les informations d'identification doivent être celles de l'administrateur du service d'abonnement ou du compte à la demande vCloud Air.

Le format du nom d'utilisateur est *domain\username*.

Fournissez des informations d'identification d'un administrateur d'organisation disposant de droits de connexion à l'aide de VMware Remote Console.

6 (Facultatif) Cliquez sur **Propriétés** et ajoutez des propriétés personnalisées fournies, des groupes de propriétés ou vos propres définitions de propriétés pour le point de terminaison.

7 (Facultatif) Pour configurer une sécurité supplémentaire et forcer les connexions à transiter par un serveur proxy, cliquez sur **Associations** et établissez une association à un point de terminaison proxy existant.

Vous devez disposer d'au moins un point de terminaison proxy pour créer une association.

8 Cliquez sur **OK**.

Suivant

[Créer un groupe Fabric.](#)

Créez un point de terminaison vCloud Director .

Vous pouvez créer un point de terminaison vCloud Director pour gérer l'ensemble des centres de données virtuels (vDC) vCloud Director de votre environnement, ou vous pouvez créer des points de terminaison distincts pour gérer chaque organisation vCloud Director. Vous pouvez éventuellement associer les paramètres de proxy au point de terminaison vCloud Director par association à un point de terminaison proxy.

Pour obtenir des informations sur les vDC d'organisation, reportez-vous à la documentation de vCloud Director.

Ne créez pas point de terminaison unique et des points de terminaison d'organisation individuels pour la même instance de vCloud Director.

vRealize Automation utilise un agent proxy pour gérer les ressources vSphere.

Remarque Les réservations définies pour les points de terminaison vCloud Air et vCloud Director ne prennent pas en charge l'utilisation de profils réseau pour le provisionnement des machines.

Pour plus d'informations sur l'association des paramètres de proxy à votre point de terminaison, reportez-vous à la section [Créer un point de terminaison proxy et l'associer à un point de terminaison cloud](#).

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur laaS**.

- Si vous souhaitez configurer une sécurité supplémentaire et forcer les connexions à transiter par un serveur proxy, créez un point de terminaison proxy. Vous pouvez associer au point de terminaison proxy lors de la création du point de terminaison vCloud Director. Reportez-vous à [Créer un point de terminaison proxy et l'associer à un point de terminaison cloud](#).

Procédure

- 1 Sélectionnez **Infrastructure > Points de terminaison > Points de terminaison**.
- 2 Sélectionnez **Nouveau > Cloud > vCloud Director**.
- 3 Entrez un nom et, éventuellement, une description.
- 4 Entrez l'URL du serveur vCloud Director dans la zone de texte **Adresse**.
L'URL doit être du type *nom de domaine complet* ou *IP_address*.
Par exemple, <https://mycompany.com>.
- 5 Entrez votre nom d'utilisateur de niveau administrateur et votre mot de passe.
 - Pour vous connecter au serveur vCloud Director et spécifier l'organisation pour laquelle l'utilisateur a le rôle d'administrateur, utilisez les informations d'identification de l'administrateur de l'organisation. En utilisant ces informations d'identification, le point de terminaison peut accéder uniquement aux centres de données virtuels associés de l'organisation. Vous pouvez ajouter des points de terminaison pour chaque organisation supplémentaire dans l'instance de vCloud Director pour les intégrer à vRealize Automation.
 - Pour permettre l'accès à tous les centres de données de l'organisation dans l'instance de vCloud Director, utilisez les informations d'identification de l'administrateur système pour vCloud Director et laissez la zone de texte **Organisation** vide.
- 6 Si vous êtes un administrateur d'organisation, vous pouvez entrer un nom d'organisation vCloud Director dans la zone de texte **Organisation**.

Option	Description
Découvrir tous les vCD d'organisation	Si vous avez mis en œuvre vCloud Director dans un cloud privé, vous pouvez laisser la zone de texte Organisation vide pour permettre à l'application de découvrir tous les vDC d'organisation disponibles.
Séparer les points de terminaison pour chaque vCD d'organisation	Entrez le nom d'une organisation vCloud Director dans la zone de texte Organisation .

Le nom de l'**Organisation** correspond au nom de votre vCloud Director organisation qui peut également s'afficher comme étant le nom de votre centre de données virtuel (vDC). Si vous utilisez un Virtual Private Cloud, ce nom est alors un identifiant unique au format M123456789-12345. Dans un cloud dédié, il s'agit du nom donné au centre de données virtuel cible.

Pour vous connecter directement à vCloud Director au niveau du système, par exemple en laissant le champ Organisation vide, vous avez besoin des informations d'identification de l'administrateur système. Si vous entrez une organisation dans le point de terminaison, vous avez besoin d'un utilisateur disposant des informations d'identification de l'administrateur de cette organisation.

Fournissez des informations d'identification disposant de droits de connexion à l'aide de VMware Remote Console.

- Pour gérer toutes les organisations avec un seul point de terminaison, fournissez des informations d'identification d'administrateur système.
- Pour gérer chaque centre de données virtuel (vDC) d'une organisation avec un point de terminaison distinct, créez des informations d'identification d'administrateur d'organisation distinctes pour chaque vDC.

Ne créez pas de point de terminaison unique au niveau du système et des points de terminaison d'organisation individuels pour la même instance de vCloud Director.

- 7 (Facultatif) Cliquez sur **Propriétés** et ajoutez des propriétés personnalisées fournies, des groupes de propriétés ou vos propres définitions de propriétés pour le point de terminaison.
- 8 (Facultatif) Pour configurer une sécurité supplémentaire et forcer les connexions à transiter par un serveur proxy, cliquez sur **Associations** et établissez une association à un point de terminaison proxy existant.

Vous devez disposer d'au moins un point de terminaison proxy pour créer une association.

- 9 Cliquez sur **OK**.

Suivant

[Créer un groupe Fabric.](#)

Créer un point de terminaison Amazon

Vous pouvez créer un point de terminaison pour vous connecter à une instance d'Amazon. Vous pouvez éventuellement associer les paramètres de proxy au point de terminaison Amazon en associant ce dernier à un point de terminaison proxy.

vRealize Automation fournit plusieurs types d'instances d'Amazon que vous pouvez utiliser lors de la création de Blueprints. Si vous souhaitez importer vos propres types d'instances, reportez-vous à la section [Ajouter un type d'instance Amazon](#).

Pour plus d'informations sur l'association des paramètres de proxy à votre point de terminaison, reportez-vous à la section [Créer un point de terminaison proxy et l'associer à un point de terminaison cloud](#).

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur IaaS**.
- Si vous souhaitez configurer une sécurité supplémentaire et forcer les connexions à transiter par un serveur proxy, créez un point de terminaison proxy. Lorsque vous créez le point de terminaison Amazon, vous pouvez l'associer au point de terminaison proxy. Reportez-vous à [Créer un point de terminaison proxy et l'associer à un point de terminaison cloud](#).

Procédure

- 1 Sélectionnez **Infrastructure > Points de terminaison > Points de terminaison**.
- 2 Sélectionnez **Nouveau > Cloud > Amazon EC2**.

- 3 Entrez un nom et, éventuellement, une description.

Ce nom indique généralement le compte Amazon qui correspond à ce point de terminaison.

- 4 Entrez l'identifiant de clé d'accès de niveau administratif pour le point de terminaison Amazon.

Vous ne pouvez associer qu'un seul point de terminaison à un identifiant de clé d'accès Amazon.

Pour obtenir la clé d'accès nécessaire à la création du point de terminaison Amazon, vous devez demander une clé à un utilisateur disposant d'informations d'identification d'administrateur ayant un accès complet à AWS ou être également configuré avec la stratégie d'administrateur avec accès complet à AWS. Pour plus d'informations, reportez-vous à la documentation d'Amazon.

- 5 Entrez la clé d'accès secrète pour le point de terminaison Amazon.

- 6 (Facultatif) Cliquez sur **Propriétés** et ajoutez des propriétés personnalisées fournies, des groupes de propriétés ou vos propres définitions de propriétés pour le point de terminaison.

- 7 (Facultatif) Pour configurer une sécurité supplémentaire et forcer les connexions à transiter par un serveur proxy, cliquez sur **Associations** et établissez une association à un point de terminaison proxy existant.

Vous devez disposer d'au moins un point de terminaison proxy pour créer une association.

- 8 Cliquez sur **OK**.

Après la création du point de terminaison, vRealize Automation commence à collecter des données depuis les régions Amazon Web Services.

Suivant

Ajoutez des ressources de calcul à partir de votre point de terminaison dans un groupe Fabric. Reportez-vous à [Créer un groupe Fabric](#).

Ajouter un type d'instance Amazon

vRealize Automation fournit plusieurs types d'instances à utiliser avec les Blueprints Amazon. Un administrateur peut ajouter et supprimer plusieurs types d'instances.

Les types d'instances de la machine gérés par les administrateurs IaaS sont mis à disposition des architectes de Blueprint lorsqu'ils créent ou modifient un Blueprint Amazon. Les images et les types d'instances de la machine Amazon sont mis à disposition par le biais du produit Amazon Web Services.

Prérequis

Connectez-vous à la console de vRealize Automation en tant qu'**administrateur IaaS**.

Procédure

- 1 Cliquez sur **Infrastructure > Administration > Types d'instances**.
- 2 Cliquez sur **Nouveau**.

3 Ajoutez un nouveau type d'instance en spécifiant les paramètres à suivre.

Pour en savoir plus sur les types d'instances d'Amazon et les valeurs de paramètres que vous pouvez spécifier, reportez-vous à la documentation d'Amazon Web Services (AWS) dans *Types d'instances EC2 - Amazon Web Services (AWS)* sur le site [Web aws.amazon.com/ec2](http://aws.amazon.com/ec2) et *Types d'instances* sur le site [Web docs.aws.amazon.com](http://docs.aws.amazon.com).

- Nom
- Nom de l'API
- Nom du type
- Nom des performances d'E/S
- CPU
- Mémoire (Go)
- Stockage (Go)
- Unités de calcul

4 Cliquez sur l'icône **Enregistrer** (✓).

Lorsque les architectes IaaS créeront des Blueprints Amazon Web Services, ils pourront utiliser les types d'instances personnalisées que vous avez créées.

Suivant

Ajoutez des ressources de calcul à partir de votre point de terminaison dans un groupe Fabric. Reportez-vous à [Créer un groupe Fabric](#).

Créer un point de terminaison proxy et l'associer à un point de terminaison cloud

Vous pouvez créer un point de terminaison proxy et associer ses paramètres de proxy à un point de terminaison vCloud Air, vCloud Director ou Amazon.

Si vous avez mis à niveau ou migré un point de terminaison vCloud Air, vCloud Director ou Amazon qui utilisait un gestionnaire de proxy, un nouveau point de terminaison vCloud Air, vCloud Director ou Amazon est créé qui contient une association entre le point de terminaison vCloud Air, vCloud Director ou Amazon et un nouveau point de terminaison proxy.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur IaaS**.
- Créez l'un des types de point de terminaison suivants :
 - [Créez un point de terminaison vCloud Air](#).
 - [Créer un point de terminaison Amazon](#)
 - [Créez un point de terminaison vCloud Director](#).

Vous devez disposer d'au moins un point de terminaison vCloud Air, vCloud Director ou Amazon pour créer une association à partir du point de terminaison proxy.

Procédure

- 1 Sélectionnez **Infrastructure > Points de terminaison > Points de terminaison**.
 - 2 Sélectionnez **Nouveau > Réseau et sécurité > Proxy**.
 - 3 Entrez un nom dans la zone de texte **Nom**.
 - 4 (Facultatif) Entrez une description dans la zone de texte **Description**.
 - 5 Entrez l'URL de l'agent proxy installé dans la zone de texte **Adresse**.
 - 6 Entrez le numéro du port qui doit être utilisé pour se connecter au serveur proxy dans la zone de texte **Port**.
 - 7 Entrez votre nom d'utilisateur de niveau administrateur et votre mot de passe.
 - 8 (Facultatif) Cliquez sur **Propriétés** et ajoutez des propriétés personnalisées fournies, des groupes de propriétés ou vos propres définitions de propriétés pour le point de terminaison.
 - 9 Pour associer les paramètres de proxy à un point de terminaison vCloud Air, vCloud Director ou Amazon, cliquez sur **Associations** et sélectionnez un ou plusieurs points de terminaison.
- Vous devez disposer d'au moins un point de terminaison vCloud Air, vCloud Director ou Amazon pour créer une association.
- Vous pouvez associer le point de terminaison proxy à plusieurs points de terminaison.
- 10 Cliquez sur **OK**.

vRealize Automation collecte les données de votre point de terminaison et détecte vos ressources de calcul.

Suivant

Ajoutez des ressources de calcul à partir de votre point de terminaison dans un groupe Fabric. Reportez-vous à [Créer un groupe Fabric](#).

Créez un point de terminaison vRealize Orchestrator .

Vous pouvez créer un point de terminaison vRealize Orchestrator pour vous connecter à un serveur vRealize Orchestrator.

Vous pouvez configurer plusieurs points de terminaison à connecter à différents serveurs vRealize Orchestrator, mais vous devez configurer une priorité pour chaque point de terminaison.

Lorsque vous exécutez des workflows vRealize Orchestrator, vRealize Automation essaie d'abord le point de terminaison vRealize Orchestrator dont la priorité est la plus élevée. Si ce point de terminaison n'est pas accessible, il passe au point de terminaison dont la priorité est la plus proche jusqu'à ce qu'un serveur vRealize Orchestrator soit disponible pour exécuter le workflow.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur laaS**.

Procédure

1 Sélectionnez **Infrastructure > Points de terminaison > Points de terminaison**.

2 Sélectionnez **Nouveau > Orchestration > vRealize Orchestrator**.

3 Entrez un nom et, éventuellement, une description.

4 Saisissez une URL avec le nom complet ou l'adresse IP du serveur vRealize Orchestrator et le numéro de port de vRealize Orchestrator.

Le protocole de transport doit être HTTPS. Si aucun port n'est spécifié, le port 443 par défaut est utilisé.

Pour utiliser l'instance de vRealize Orchestrator par défaut intégrée au dispositif vRealize Automation, tapez **https://vrealize-automation-appliance-hostname:443/vco**.

5 Fournissez vos informations d'identification vRealize Orchestrator dans les zones de texte **Nom d'utilisateur** et **Mot de passe** pour vous connecter au point de terminaison vRealize Orchestrator.

Les informations d'identification que vous utilisez doivent disposer d'autorisations d'exécution pour tous les workflows vRealize Orchestrator que vous appelez depuis l'laaS.

Pour utiliser l'instance de vRealize Orchestrator par défaut intégrée au dispositif vRealize Automation, le nom d'utilisateur est **administrator@vsphere.local** et le mot de passe est le mot de passe d'administrateur spécifié lors de la configuration de SSO.

6 Saisissez un entier supérieur ou égal à 1 dans la zone de texte **Priorité**.

Une valeur inférieure indique une priorité plus élevée.

7 (Facultatif) Cliquez sur **Propriétés** et ajoutez des propriétés personnalisées fournies, des groupes de propriétés ou vos propres définitions de propriétés pour le point de terminaison.

8 Cliquez sur **OK**.

Configuration de points de terminaison vRealize Orchestrator pour la mise en réseau

Si vous utilisez des workflows vRealize Automation pour appeler des workflows vRealize Orchestrator, vous devez configurer l'instance ou le serveur de vRealize Orchestrator en tant que point de terminaison.

Pour plus d'informations sur l'ajout d'un point de terminaison vRealize Orchestrator, reportez-vous à [Créez un point de terminaison vRealize Orchestrator](#).

Vous pouvez associer un point de terminaison vRealize Orchestrator à un Blueprint de machine pour vous assurer que tous les workflows vRealize Orchestrator des machines provisionnées à partir de ce Blueprint s'exécutent à l'aide de ce point de terminaison.

Par défaut, vRealize Automation inclut une instance de vRealize Orchestrator intégrée. Nous vous recommandons de l'utiliser comme votre point de terminaison vRealize Orchestrator pour l'exécution de workflows vRealize Automation dans un environnement de test ou en tant que validation technique.

Il est également recommandé d'utiliser ce point de terminaison vRealize Orchestrator pour exécuter des workflows vRealize Automation dans un environnement de production.

Le plug-in vRealize Orchestrator est automatiquement installé avec vRealize Orchestrator 7.1 et versions ultérieures. Il n'existe aucun plug-in vRealize Orchestrator distinct à installer.

Créer un point de terminaison vRealize Operations Manager

Vous pouvez créer un point de terminaison vRealize Operations Manager pour vous connecter à une API de suite d'hôtes vRealize Operations Manager.

Pour plus d'informations sur la validation de la connexion vRealize Operations Manager et l'approbation du certificat, reportez-vous à la section [Considérations sur l'utilisation du test des connexions](#).

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur laaS**.

Procédure

- 1 Sélectionnez **Infrastructure > Points de terminaison > Points de terminaison**.
- 2 Sélectionnez **Nouveau > Gestion > vRealize Operations Manager**.
- 3 Entrez un nom et, éventuellement, une description.
- 4 Entrez l'URL du serveur vRealize Operations Manager dans la zone de texte **Adresse**.
L'URL doit être au format : **https://hostname/suite-api**.
- 5 Entrez votre nom d'utilisateur vRealize Operations Manager et votre mot de passe.
- 6 (Facultatif) Cliquez sur **Propriétés** et ajoutez des propriétés personnalisées fournies, des groupes de propriétés ou vos propres définitions de propriétés pour le point de terminaison.
- 7 (Facultatif) Cliquez sur **Tester la connexion** pour valider les informations d'identification, l'adresse de point de terminaison d'hôte et le certificat de confiance. L'action vérifie également que Service Manager et l'agent sont en cours d'exécution afin que le point de terminaison puisse faire l'objet d'une collecte de données. L'action **OK** teste ces mêmes conditions.

L'action de **Tester la connexion** renvoie des informations sur une des conditions suivantes :

- Erreur de certificat
Si le certificat n'est pas trouvé, n'est pas approuvé ou a expiré, vous êtes invité à accepter une empreinte numérique de certificat. Si vous n'acceptez pas l'empreinte numérique, vous pouvez toujours enregistrer le point de terminaison, mais le provisionnement de la machine peut échouer.
- Erreur de l'agent
L'agent vSphere associé est introuvable. L'agent doit être en cours d'exécution pour que le test réussisse.
- Erreur de l'hôte
L'adresse de point de terminaison spécifiée n'est pas accessible ou l'instance associée de Manager Service n'est pas en cours d'exécution. Manager Service doit être en cours d'exécution pour que le test réussisse.

- Erreur d'informations d'identification

La combinaison du nom d'utilisateur et du mot de passe spécifiée n'est pas valide pour le point de terminaison à l'adresse spécifiée.

- Délai d'expiration

L'action de test n'a pas pu aboutir dans le délai imparti de deux minutes.

Si l'action **Tester la connexion** échoue, vous pouvez toujours enregistrer le point de terminaison, mais le provisionnement de la machine risque d'échouer.

S'il y a un problème de certificat approuvé, par exemple le certificat a expiré, un message vous invite à accepter une empreinte de certificat.

8 Cliquez sur **OK**.

Créer un point de terminaison de fournisseur IPAM tiers

Si vous avez enregistré et configuré un type de point de terminaison IPAM tiers dans vRealize Orchestrator, vous pouvez créer un point de terminaison pour ce fournisseur de solutions IPAM dans vRealize Automation.

Si vous avez importé un module vRealize Orchestrator pour provisionner une solution IPAM externe et enregistré le type de point de terminaison IPAM dans vRealize Orchestrator, vous pouvez sélectionner ce type de point de terminaison IPAM lorsque vous créez un point de terminaison vRealize Automation.

Remarque Cet exemple est basé sur l'utilisation du plug-in Infoblox IPAM, qui peut être téléchargé dans VMware Solution Exchange. Vous pouvez également utiliser cette procédure si vous avez créé votre propre module de fournisseur IPAM à l'aide du SDK de solutions IPAM fourni par VMware. La procédure d'importation et de configuration de votre propre module de solution IPAM tiers est la même que celle décrite dans les conditions préalables.

Le premier point de terminaison IPAM pour vRealize Automation est créé lorsque vous enregistrez le type de point de terminaison pour le plug-in du fournisseur de solutions IPAM dans vRealize Orchestrator.

Prérequis

- [Obtenir et importer un module de fournisseur IPAM tiers dans vRealize Orchestrator.](#)
- [Exécuter un workflow pour enregistrer un type de point de terminaison IPAM tiers dans vRealize Orchestrator.](#)
- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur laaS**.

Pour cet exemple, créez un point de terminaison Infoblox IPAM en utilisant un type de point de terminaison que vous avez enregistré dans vRealize Orchestrator pour votre plug-in de fournisseur ou module IPAM tiers importé.

Procédure

1 Sélectionnez **Infrastructure > Points de terminaison > Points de terminaison**.

2 Sélectionnez **Nouveau > IPAM > Type de point de terminaison IPAM**.

Sélectionnez un type de point de terminaison de fournisseur IPAM tel qu'Infoblox. Les points de terminaison de fournisseur IPAM externe sont uniquement disponibles si vous avez importé un module vRealize Orchestrator tiers, et exécuté les workflows du module pour enregistrer le type de point de terminaison.

Pour Infoblox IPAM, seuls les types de point de terminaison IPAM principaux sont répertoriés. Vous pouvez spécifier des types de point de terminaison IPAM secondaires en utilisant des propriétés personnalisées.

Pour cet exemple, sélectionnez un type de point de terminaison IPAM externe enregistré, par exemple **Infoblox NIOS**.

3 Entrez un nom et, éventuellement, une description.

4 Entrez l'emplacement du point de terminaison IPAM enregistré dans la zone de texte **Adresse** en utilisant le format URL spécifique au fournisseur, par exemple `https://host_name/name`.

Par exemple, vous pouvez créer plusieurs points de terminaison IPAM, tels que `https://nsx62-scale-infoblox` et `https://nsx62-scale-infoblox2`, lorsque vous enregistrez le type de point de terminaison IPAM dans vRealize Orchestrator. Entrez un type de point de terminaison enregistré principal. Pour également spécifier un ou plusieurs points de terminaison IPAM secondaires, vous pouvez utiliser des propriétés personnalisées pour émuler des attributs extensibles qui sont spécifiques au fournisseur de solutions IPAM.

5 Entrez le nom d'utilisateur et le mot de passe requis pour accéder au compte du fournisseur de solutions IPAM.

Les informations d'identification du compte du fournisseur de solutions IPAM sont requises pour créer, configurer et modifier le point de terminaison lors d'un travail dans vRealize Automation. vRealize Automation utilise les informations d'identification du point de terminaison IPAM pour communiquer avec le type de point de terminaison spécifié, par exemple Infoblox, pour attribuer des adresses IP et effectuer d'autres opérations. Ce comportement est similaire à la manière dont vRealize Automation utilise les informations d'identification de point de terminaison vSphere.

6 (Facultatif) Cliquez sur **Propriétés** et ajoutez des propriétés de point de terminaison qui sont significatives pour le fournisseur de solutions IPAM spécifique.

Chaque fournisseur de solutions IPAM, par exemple Infoblox et Bluecat, utilise des attributs extensibles que vous pouvez émuler en utilisant des propriétés personnalisées vRealize Automation. Par exemple, Infoblox utilise des attributs extensibles pour différencier les points de terminaison principaux et secondaires.

7 Cliquez sur **OK**.

Suivant

Ajoutez des ressources de calcul à partir de votre point de terminaison dans un groupe Fabric. Reportez-vous à [Créer un groupe Fabric](#).

Créer un point de terminaison Microsoft Azure

Vous pouvez créer un point de terminaison Microsoft Azure pour faciliter une connexion avec informations d'identification entre vRealize Automation et un déploiement Azure.

Un point de terminaison établit une connexion à une ressource, dans ce cas une instance d'Azure, que vous pouvez utiliser pour créer des Blueprints de machine virtuelle. Vous devez disposer d'un point de terminaison Azure comme base des Blueprints pour le provisionnement de machines virtuelles Azure. Si vous utilisez plusieurs abonnements Azure, des points de terminaison seront nécessaires pour chaque ID d'abonnement.

Vous pouvez également créer une connexion Azure directement à partir de vRealize Orchestrator en utilisant la commande d'ajout d'une connexion Azure située sous **Bibliothèque > Azure > Configuration** dans l'arborescence du workflow vRealize Orchestrator. Dans la plupart des cas, il est recommandé de créer une connexion en configurant des points de terminaison comme décrit dans le présent document.

Les points de terminaison Azure sont pris en charge par vRealize Orchestrator et par la fonctionnalité XaaS. Vous pouvez créer, supprimer ou modifier un point de terminaison Azure. Notez que si vous apportez des modifications à un point de terminaison existant et n'exécutez pas de mises à jour sur le portail Azure via la connexion mise à jour pendant plusieurs heures, vous devez redémarrer le service vRealize Orchestrator à l'aide de la commande `service vco-service restart`. Le fait de ne pas redémarrer le service risque de provoquer des erreurs.

Prérequis

- Configurez une instance de Microsoft Azure et obtenez un abonnement valide à Microsoft Azure à partir duquel vous pouvez utiliser l'ID d'abonnement. Reportez-vous à <http://www.vaficionado.com/2016/11/using-new-microsoft-azure-endpoint-vrealize-automation-7-2/> pour plus d'informations sur la configuration d'Azure et l'obtention d'un ID d'abonnement.
- Votre déploiement vRealize Automation doit comporter au moins un locataire et un groupe d'activité.
- Créez une application Active Directory comme indiqué dans <https://azure.microsoft.com/fr-fr/documentation/articles/resource-group-create-service-principal-portal>.
- Prenez note des informations suivantes concernant Azure. Vous en aurez besoin lors de la configuration des points de terminaison et des Blueprints.
 - ID de l'abonnement
 - ID du locataire
 - nom du compte de stockage
 - nom du groupe de ressources
 - emplacement
 - nom du réseau virtuel
 - ID de l'application cliente
 - clé secrète de l'application cliente
 - image de machine virtuelle URN

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

- 1 Sélectionnez **Administration > Points de terminaison > Points de terminaison Orchestrator**.
- 2 Cliquez sur l'icône **Nouveau** (+).
- 3 Dans l'onglet Plug-in, cliquez sur le menu déroulant **Plug-in** et sélectionnez Plug-in Azure.
- 4 Cliquez sur **Suivant**.
- 5 Entrez un nom et, éventuellement, une description.
- 6 Cliquez sur **Suivant**.
- 7 Renseignez les zones de texte dans l'onglet **Détails** en fonction du point de terminaison.

Paramètre	Description
Paramètres de connexion	
Connexion Azure	
Nom de la connexion	Nom unique de la connexion du nouveau point de terminaison. Ce nom figure dans l'interface de vRealize Orchestrator pour vous aider à identifier une connexion particulière.
ID d'abonnement Azure	Identifiant de votre abonnement Azure. L'ID définit les comptes de stockage, les machines virtuelles et autres ressources Azure auxquelles vous avez accès.
Paramètres du Gestionnaire de ressources	
URI du service Azure	L'URI par lequel vous pouvez accéder à votre instance d'Azure. La valeur par défaut <code>https://management.azure.com/</code> convient à de nombreuses implémentations type.
ID de locataire	ID du locataire Azure que vous souhaitez que le point de terminaison utilise.
ID client	ID du client Azure que vous souhaitez que le point de terminaison utilise. Ceci est affecté lorsque vous créez une application Active Directory.
Clé secrète client	La clé utilisée avec un ID client Azure. Cette clé est affectée lorsque vous créez une application Active Directory.
URL de connexion	URL utilisée pour accéder à l'instance d'Azure. La valeur par défaut <code>https://login.windows.net/</code> convient à de nombreuses implémentations type.
Paramètres du proxy	
Hôte proxy	Si votre organisation utilise un serveur proxy Web, entrez le nom d'hôte de ce serveur.
Port du proxy	Si votre organisation utilise un serveur proxy Web, entrez le numéro de port de ce serveur.

8 Cliquez sur **Terminer**.

Suivant

Créez des groupes de ressources, des comptes de stockage et des groupes de sécurité réseau Azure appropriés. Vous devez également créer des équilibres de charge si approprié pour votre implémentation.

Action	Options
Créer un groupe de ressources Azure	<ul style="list-style-type: none"> ■ Créez le groupe de ressources à l'aide du portail Azure. Reportez-vous à la documentation d'Azure pour obtenir des instructions spécifiques. ■ Utilisez le workflow vRealize Orchestrator approprié se trouvant sous le groupe de ressources <code>Library/Azure/Resource/Create</code>. ■ Dans vRealize Automation, créez et publiez un Blueprint XaaS contenant le workflow vRealize Orchestrator. Vous pouvez demander le groupe de ressources après son attachement au service et aux droits. Notez que le type de ressource du groupe de ressources n'est pas pris en charge ou géré par vRealize Automation.
Créer un compte de stockage Azure	<ul style="list-style-type: none"> ■ Utilisez Azure pour créer un compte de stockage. Reportez-vous à la documentation d'Azure pour obtenir des instructions spécifiques. ■ Utilisez le workflow vRealize Orchestrator approprié se trouvant sous le compte de stockage <code>Library/Azure/Storage/Create storage account</code>. ■ Dans vRealize Automation, créez et publiez un Blueprint XaaS contenant le workflow vRealize Orchestrator. Vous pouvez demander le compte de stockage après son attachement au service et aux droits.
Créer un groupe de sécurité réseau Azure	<ul style="list-style-type: none"> ■ Utilisez Azure pour créer un groupe de sécurité. Reportez-vous à la documentation d'Azure pour obtenir des instructions spécifiques. ■ Utilisez le workflow vRealize Orchestrator approprié se trouvant dans le groupe de sécurité <code>Library/Azure/Network/Create</code>. ■ Dans vRealize Automation, créez et publiez un Blueprint XaaS contenant le workflow vRealize Orchestrator. Vous pouvez demander le groupe de sécurité après son attachement au service et aux droits.

Créer un point de terminaison Puppet

Vous pouvez créer un point de terminaison Puppet pour prendre en charge l'ajout de composants de gestion de configuration Puppet à des machines virtuelles vSphere. Ces composants vous permettent d'utiliser un serveur Puppet Master pour appliquer la gestion de la configuration aux machines virtuelles.

Un point de terminaison établit une connexion à une ressource externe, dans le cas présent une instance du serveur Puppet Master. Le point de terminaison vous permet de placer des composants de gestion de configuration Puppet sur des Blueprints de machine virtuelle vSphere. Les machines virtuelles provisionnées en fonction de ces Blueprints contiennent un agent Puppet qui facilite le contrôle par le serveur Puppet Master associé.

Prérequis

- Installez et configurez Puppet Enterprise d'une façon adaptée à votre environnement.
- Téléchargez et installez la version 3.0 du plug-in Puppet sur votre déploiement de vRealize Orchestrator. Vous pouvez télécharger ce plug-in sur <https://solutionexchange.vmware.com/store/products/puppet-plugin-for-vrealize-automation>. Pour plus d'informations sur l'installation et l'utilisation du plug-in, reportez-vous à la section https://docs.puppet.com/pe/latest/vro_intro.html.

Procédure

- 1 Sélectionnez **Administration > Points de terminaison > Points de terminaison Orchestrator**.
- 2 Cliquez sur l'icône **Nouveau** (+).
- 3 Dans l'onglet Plug-in, cliquez sur le menu déroulant **Plug-in** et sélectionnez **Plug-in Puppet**.
- 4 Cliquez sur **Suivant**.
- 5 Entrez un nom et, éventuellement, une description.
- 6 Cliquez sur **Suivant**.
- 7 Renseignez les zones de texte dans l'onglet **Détails** en fonction du point de terminaison.

Paramètre	Description
Nom d'affichage de ce serveur Puppet Master	Nom du serveur Puppet Master associé à la connexion du point de terminaison. Ce nom figure dans l'interface de vRealize Orchestrator pour vous aider à identifier une connexion particulière.
Nom d'hôte ou adresse IP	Nom de domaine complet ou adresse IP du serveur Puppet Master utilisé par ce point de terminaison.
Port SSH	Port défini pour une utilisation avec une communication sécurisée pour ce serveur Puppet Master.
RBAC SSH et nom d'utilisateur	Nom d'utilisateur du contrôle d'accès basé sur les rôles requis pour la connexion au serveur Puppet Master.
SSH et mot de passe RBAC	Nom d'utilisateur du contrôle d'accès basé sur les rôles requis pour une configuration sécurisée avec le serveur Puppet Master.
Utiliser sudo pour les commandes shell sur ce master ?	Sélectionnez cette option si vous souhaitez que les administrateurs puissent utiliser les commandes Sudo sur les serveurs Linux pour les options de sécurité des machines virtuelles en fonction de ce point de terminaison.

8 Cliquez sur **OK**.

Vous pouvez maintenant ajouter des composants de gestion de configuration Puppet à des Blueprints vSphere afin de pouvoir déployer des machines virtuelles vSphere contenant des agents Puppet.

Créer un point de terminaison Hyper-V (SCVMM)

Vous pouvez créer des points de terminaison pour permettre à vRealize Automation de communiquer avec votre environnement SCVMM et découvrir les ressources de calcul, collecter les données et provisionner les machines.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur laaS**.
- Pour gérer votre point de terminaison Hyper-V (SCVMM), vous devez installer et configurer un agent DEM. Pour plus d'informations, reportez-vous à la rubrique Conditions requises de SCVMM dans *Installation de vRealize Automation 7.3*

Pour des informations complémentaires, reportez-vous à [Préparation de votre environnement SCVMM](#).

Procédure

- 1 Sélectionnez **Infrastructure > Points de terminaison > Points de terminaison**.
- 2 Sélectionnez **Nouveau > Virtuel > Hyper-V (SCVMM)**.
- 3 Entrez un nom dans la zone de texte **Nom**.
- 4 (Facultatif) Entrez une description dans la zone de texte **Description**.
- 5 Entrez l'URL du point de terminaison dans la zone de texte **Adresse**.
L'URL doit être du type : *nom_de_domaine_complet* ou *adresse_IP*.
Par exemple : `monentreprise-scvmm1.monentreprise.local`.
- 6 Entrez le nom d'utilisateur de niveau administratif et le mot de passe que vous avez stocké pour ce point de terminaison.
Si vous n'avez pas encore stocké les informations d'identification, vous pouvez le faire maintenant.
- 7 (Facultatif) Cliquez sur **Propriétés** et ajoutez des propriétés personnalisées fournies, des groupes de propriétés ou vos propres définitions de propriétés pour le point de terminaison.
- 8 Cliquez sur **OK**.

vRealize Automation collecte les données de votre point de terminaison et détecte vos ressources de calcul.

Suivant

Ajoutez des ressources de calcul à partir de votre point de terminaison dans un groupe Fabric. Reportez-vous à [Créer un groupe Fabric](#).

Créer un point de terminaison OpenStack

Vous créez un point de terminaison pour autoriser vRealize Automation à communiquer avec votre instance d'OpenStack.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur IaaS**.
- Vérifiez que vos DEM vRealize Automation sont installés sur une machine répondant à la configuration requise d'Openstack ou de PowerVC. Reportez-vous à *Installation de vRealize Automation 7.3*.
- Vérifiez que votre variante d'Openstack est actuellement prise en charge. Reportez-vous à *Matrice de prise en charge de vRealize Automation*.

Après avoir effectué une mise à niveau ou une migration à partir d'une installation antérieure à vRealize Automation, si la collecte de données échoue pour les points de terminaison OpenStack, vous pouvez ajouter la propriété personnalisée

`VMware.Endpoint.Openstack.IdentityProvider.Domain.Name` à chaque point de terminaison Keystone V3 OpenStack pour spécifier un nom de domaine valide et activer la collecte de données.

Procédure

- 1 Sélectionnez **Infrastructure > Points de terminaison > Points de terminaison**.
- 2 Sélectionnez **Nouveau > Cloud > OpenStack**.
- 3 Entrez un nom et, éventuellement, une description.
- 4 Entrez l'URL du point de terminaison dans la zone de texte **Adresse**.

Option	Description
PowerVC	L'URL doit avoir le format http://myPowerVC.com:5000 ou http://FQDN:5000 .
Openstack	Le format de l'URL doit être nom_de_domaine_complet:5000 ou adresse_IP:5000 . N'incluez pas le suffixe /v2.0 dans l'adresse du point de terminaison.

- 5 Entrez votre nom d'utilisateur de niveau administratif et votre mot de passe.

Les informations d'identification que vous fournissez doivent avoir le rôle d'administrateur dans le locataire OpenStack associé au point de terminaison.
- 6 Entrez un nom de locataire OpenStack dans la zone de texte **Projet OpenStack**.

Si vous configurez plusieurs points de terminaison avec des locataires OpenStack différents, créez des stratégies de réservation pour chaque locataire. Cela garantit que les machines sont allouées aux ressources de locataire appropriées.

- 7 Cliquez sur **Propriétés** et ajoutez des propriétés personnalisées fournies, des groupes de propriétés ou vos propres définitions de propriétés pour le point de terminaison.

Si Keystone V3 est en vigueur, ajoutez la propriété personnalisée `VMware.Endpoint.Openstack.IdentityProvider.Domain.Name` pour désigner un domaine spécifique.

- 8 Cliquez sur **OK**.

vRealize Automation collecte les données de votre point de terminaison et détecte vos ressources de calcul.

Suivant

Ajoutez des ressources de calcul à partir de votre point de terminaison dans un groupe Fabric. Reportez-vous à [Créer un groupe Fabric](#).

Créer un point de terminaison Hyper-V, XenServer ou de pool Xen

Vous pouvez créer des points de terminaison pour permettre à vRealize Automation de communiquer avec l'environnement Hyper-V, XenServer ou du serveur maître du pool Xen, et découvrir les ressources de calcul, collecter les données et provisionner les machines.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur IaaS**.
- Un administrateur système doit installer un agent proxy avec des informations d'identification stockées qui correspond à votre point de terminaison. Reportez-vous à *Installation de vRealize Automation 7.3*.

Procédure

- 1 Sélectionnez **Infrastructure > Points de terminaison > Agents**.
- 2 Entrez le nom DNS complet du serveur Hyper-V, XenServer ou du serveur maître du pool Xen dans la zone de texte **Ressource de calcul**.

Remarque Pour un point de terminaison du pool Xen, vous devez entrer le nom du serveur maître du pool.

Pour éviter les doublons dans la table des ressources de calcul vRealize Automation, spécifiez une adresse qui corresponde à l'adresse configurée pour le serveur maître du pool Xen. Par exemple, si l'adresse du serveur maître du pool Xen utilise le nom d'hôte, entrez le nom d'hôte et pas le nom de domaine complet (FQDN, Fully Qualified Domain Name). Si l'adresse du serveur maître du pool Xen utilise le FQDN, faites de même.

- 3 Sélectionnez l'agent proxy que votre administrateur système a installé pour ce point de terminaison dans le menu déroulant **Nom de l'agent proxy**.
- 4 (Facultatif) Entrez une description dans la zone de texte **Description**.
- 5 Cliquez sur **OK**.

vRealize Automation collecte les données de votre point de terminaison et détecte vos ressources de calcul.

Suivant

Ajoutez des ressources de calcul à partir de votre point de terminaison dans un groupe Fabric. Reportez-vous à [Créer un groupe Fabric](#).

Considérations sur l'utilisation du test des connexions

Vous pouvez utiliser une action de test des connexions pour valider les informations d'identification, l'adresse du point de terminaison hôte et le certificat d'un point de terminaison vSphere, NSX ou vRealize Operations Manager.

L'action vérifie également que Service Manager et l'agent sont en cours d'exécution afin que le point de terminaison puisse faire l'objet d'une collecte de données.

L'action de **Tester la connexion** renvoie des informations sur une des conditions suivantes :

- Erreur de certificat

Si le certificat n'est pas trouvé, n'est pas approuvé ou a expiré, vous êtes invité à accepter une empreinte numérique de certificat. Si vous n'acceptez pas l'empreinte numérique, vous pouvez toujours enregistrer le point de terminaison, mais le provisionnement de la machine peut échouer.

- Erreur de l'agent

L'agent vSphere associé est introuvable. L'agent doit être en cours d'exécution pour que le test réussisse.

- Erreur de l'hôte

L'adresse de point de terminaison spécifiée n'est pas accessible ou l'instance associée de Manager Service n'est pas en cours d'exécution. Manager Service doit être en cours d'exécution pour que le test réussisse.

- Erreur d'informations d'identification

La combinaison du nom d'utilisateur et du mot de passe spécifiée n'est pas valide pour le point de terminaison à l'adresse spécifiée.

- Délai d'expiration

L'action de test n'a pas pu aboutir dans le délai imparti de deux minutes.

Si vous rencontrez des erreurs lors de l'exécution du **Test de connexion** sur les points de terminaison mis à niveau ou migrés, reportez-vous à la section [Éléments à prendre en compte lors de l'utilisation de points de terminaison mis à niveau ou migrés](#) pour les étapes nécessaires pour établir l'approbation du certificat.

Importer ou exporter des points de terminaison par programme

Pour importer et exporter des points de terminaison par programme dans vRealize Automation 7.3 ou une version ultérieure, vous devez utiliser deux nouvelles API REST endpoint-configuration-service vRealize Automation ou utiliser vRealize CloudClient.

La documentation de vRealize CloudClient contient toutes les syntaxes de ligne de commande, exemples et informations d'utilisation applicables.

Vous pouvez télécharger l'application vRealize CloudClient et la documentation à partir de la page du produit vRealize CloudClient de <https://developercenter.vmware.com/tool/cloudclient>.

Affichage des sources de point de terminaison et exécution de la collecte de données

Vous pouvez afficher la machine et la ressource de calcul qui est associée à un point de terminaison spécifique. Vous pouvez également démarrer manuellement la collecte de données.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur laaS**.
- Vérifiez qu'au moins un point de terminaison existe.

Procédure

- 1 Sélectionnez **Infrastructure > Points de terminaison > Points de terminaison**.
- 2 Sélectionnez une ligne de point de terminaison existante et cliquez sur **Actions**.

Sélectionnez l'une des actions disponibles suivantes.

- Cliquez sur **Afficher les ressources de calcul** pour ouvrir la page **Infrastructure > Ressources de calcul**. Vous pouvez utiliser cette page pour afficher et modifier les paramètres des ressources de calcul.
- Cliquez sur **Afficher les machines** pour ouvrir la page **Infrastructure > Machines gérées**.
- Cliquez sur **Collecte de données** pour ouvrir la page de collecte de données et démarrer la collecte des données pour le point de terminaison. Vous pouvez actualiser la page pour afficher l'état actuel de la demande.

Éléments à prendre en compte lors de l'utilisation de points de terminaison mis à niveau ou migrés

Après une mise à niveau ou une migration à partir d'une version antérieure à vRealize Automation 7.3, il est important de bien comprendre les éléments à prendre en compte suivants et d'agir en conséquence.

Ces informations s'appliquent aux points de terminaison qui ont été mis à niveau ou migrés vers cette version de vRealize Automation.

- Lorsque vous procédez à une mise à niveau ou à une migration à partir d'une version antérieure à vRealize Automation 7.3, chaque point de terminaison vCloud Air, vCloud Director et Amazon qui contient des paramètres de proxy est associé à un nouveau point de terminaison proxy qui contient les paramètres de proxy.

Après la mise à niveau ou la migration, le nouveau nom du point de terminaison proxy est Proxy_YYYYY où YYYYY est un hachage de l'URL du proxy, du port et des informations d'identification. Si vous utilisiez les mêmes paramètres de proxy (par exemple, la même URL, le même port et les mêmes informations d'identification) pour un point de terminaison différent (par

exemple, un point de terminaison vCloud Air ou Amazon), après la mise à niveau ou la migration, il n'y a qu'un seul point de terminaison proxy et une association entre le point de terminaison vCloud Air et Amazon et le nouveau point de terminaison proxy. Un point de terminaison proxy peut être associé à plusieurs points de terminaison Amazon, vCloud Air ou vCloud Director.

- Lorsque vous mettez à niveau ou migrez les points de terminaison vSphere qui contiennent les paramètres NSX Manager, chaque point de terminaison vSphere est associé à un nouveau point de terminaison NSX contenant ses paramètres NSX Manager.

Après la mise à niveau ou la migration, le nom du point de terminaison NSX est NSX_XXXXX, où XXXXX est le nom du point de terminaison vRealize Automation parent dans la version antérieure à vSphere 7.3.

- Lorsque la mise à niveau ou la migration de vRealize Automation est terminée, un administrateur de l'infrastructure peut modifier les nouveaux noms des points de terminaison NSX et proxy.
- Le paramètre de sécurité par défaut pour les points de terminaison mis à niveau ou migrés consiste à ne pas accepter les certificats non approuvés.
- Après la mise à niveau ou la migration à partir d'une version antérieure à vRealize Automation, si vous utilisiez des certificats non approuvés, vous devez effectuer la procédure suivante pour tous les points de terminaison vSphere et NSX afin d'activer la validation du certificat. Si vous ne le faites pas, les opérations de point de terminaison échouent et produisent des erreurs de certificat. Pour plus d'informations, consultez les articles de la base de connaissances VMware *La communication au point de terminaison est interrompue après la mise à niveau vers vRA 7.3 (2150230)* à l'adresse <http://kb.vmware.com/kb/2150230> et *Comment télécharger et installer des certificats vCenter Server racine pour éviter les avertissements de certificat de navigateur Web (2108294)* à l'adresse <http://kb.vmware.com/kb/2108294>.
 - a Après une mise à niveau ou une migration, connectez-vous à la machine de l'agent vSphere vRealize Automation et redémarrez vos agents vSphere à l'aide de l'onglet **Services**.

Il se peut que la migration ne fasse pas redémarrer tous les agents ; si tel est le cas, redémarrez-les manuellement.
 - b Attendez qu'au moins un rapport de commande ping se termine. Cette opération peut prendre une à deux minutes.
 - c Lorsque les agents vSphere ont démarré la collecte de données, connectez-vous à vRealize Automation en tant qu'administrateur IaaS.
 - d Cliquez sur **Infrastructure > Points de terminaison > Points de terminaison**.
 - e Modifiez un point de terminaison vSphere et cliquez sur **Tester la connexion**.
 - f Si une invite de certificat s'affiche, cliquez sur **OK** pour accepter le certificat.

Si aucune invite de certificat ne s'affiche, il se peut qu'actuellement le certificat soit correctement stocké dans une autorité racine approuvée du service d'hébergement de la machine Windows pour le point de terminaison, par exemple en tant que machine de l'agent proxy ou machine DEM.

- g Cliquez sur **OK** pour appliquer l'acceptation du certificat et enregistrer le point de terminaison.
- h Répétez cette procédure pour chaque point de terminaison vSphere.
- i Répétez cette procédure pour chaque point de terminaison NSX.

Si l'action **Tester la connexion** réussit, mais certaines opérations de collecte ou de provisionnement de données échouent, vous pouvez installer le même certificat sur toutes les machines de l'agent qui servent de point de terminaison et sur toutes les machines DEM. Vous pouvez également désinstaller le certificat des machines existantes et répéter la procédure précédente pour le point de terminaison défaillant.

- Les API REST de vRealize Automation qui ont été utilisées pour créer, modifier et supprimer des points de terminaison dans vRealize Automation 7.2 et versions antérieures par programmation ne sont plus prises en charge dans vRealize Automation 7.3 et versions ultérieures. Pour créer, modifier et supprimer des points de terminaison dans vRealize Automation 7.3 ou version ultérieure par programmation, vous devez utiliser deux nouvelles API REST de service de configuration de point de terminaison vRealize Automation ou utiliser vRealize CloudClient.
- Après avoir effectué une mise à niveau ou une migration à partir d'une installation antérieure à vRealize Automation, si la collecte de données échoue pour les points de terminaison OpenStack, vous pouvez ajouter la propriété personnalisée `VMware.Endpoint.Openstack.IdentityProvider.Domain.Name` à chaque point de terminaison Keystone V3 OpenStack pour spécifier un nom de domaine valide et activer la collecte de données.
- Lorsque vous mettez à niveau un point de terminaison IPAM tiers, par exemple Infoblox IPAM, le module vRealize Orchestrator contenant le workflow `RegisterIPAMEndpoint` est mis à niveau. Vous devrez éventuellement réexécuter le workflow dans vRealize Orchestrator lorsque la mise à niveau de vRealize Automation sera terminée.
- Pour modifier les informations d'identification sur plusieurs points de terminaison, vous pouvez modifier les points de terminaison individuellement ou utiliser vRealize CloudClient pour effectuer une mise à jour en bloc.
- Certains types de point de terminaison, tels que vCloud Air et vCloud Director, ne peuvent pas être mis à niveau ou migrés directement de vRealize Automation 6.2.x vers vRealize Automation 7.3 ou version supérieure.
- Après une mise à niveau ou une migration vers vRealize Automation 7.3, si la page **Infrastructure > Points de terminaison** n'affiche pas de points de terminaison ou n'affiche que certains types de point de terminaison et points de terminaison, reportez-vous à [l'article 2150252 de la base de connaissances](#) pour une suggestion de solution.

Éléments à prendre en compte lors de la suppression des points de terminaison

Vous pouvez supprimer certains types de point de terminaison sous certaines conditions.

- Vous pouvez supprimer les points de terminaison dont les données n'ont pas été collectées.
- Vous pouvez supprimer un point de terminaison OpenStack, Amazon et VRO si ses données ont été collectées, mais sans réservation. Les autres types de points de terminaison ne peuvent pas être supprimés si leurs données ont été collectées.

- Vous pouvez supprimer un point de terminaison IPAM tiers s'il n'a aucune association avec un profil réseau.
- Lorsque vous supprimez un point de terminaison vSphere, l'invite de confirmation répertorie les dépendances suivantes :
 - Le point de terminaison a fait l'objet d'une collecte de données.
 - Le point de terminaison est référencé dans une réservation qui est mappée à une ressource de calcul. Vous ne pouvez pas supprimer un point de terminaison référencé dans une réservation. Les réservations nécessitent une ressource de calcul.
 - Le point de terminaison contient un modèle qui est référencé dans un Blueprint existant. Le Blueprint n'est pas supprimé lorsque vous supprimez le point de terminaison.
 - Le point de terminaison est utilisé par des machines virtuelles en cours d'utilisation.
- Vous pouvez supprimer des points de terminaison par programme en utilisant les nouvelles API REST endpoint-configuration-service vRealize Automation CREATE, EDIT et DELETE introduites dans vRealize Automation 7.3 ou à l'aide de vRealize CloudClient. Vous ne pouvez pas supprimer des points de terminaison à l'aide des API REST endpoint-configuration-service antérieures à vRealize Automation 7.3.

Résolution du problème Impossible de trouver le point de terminaison vSphere associé

Lorsque la collecte de données échoue pour un point de terminaison vSphere, cela peut être dû à une incohérence entre le nom du proxy et le nom du point de terminaison.

Problème

La collecte de données échoue pour un point de terminaison vSphere. Les messages du journal renvoient une erreur similaire à la suivante :

```
L'exception suivante a été interceptée : impossible de trouver le point de terminaison associé
« vCenter ».
```

Cause

Le nom du point de terminaison que vous configurez dans vRealize Automation doit correspondre au nom du point de terminaison fourni à l'agent proxy vSphere lors de l'installation. La collecte de données échoue pour un point de terminaison vSphere en cas d'incohérence entre le nom du point de terminaison et le nom de l'agent proxy. Tant qu'un point de terminaison portant un nom correspondant n'est pas configuré, les messages du journal renvoient une erreur similaire à la suivante :

```
L'exception suivante a été interceptée : impossible de trouver le point de terminaison associé
'expected endpoint name'.
```

Solution

- 1 Sélectionnez **Infrastructure > Surveillance > Journal**.

- 2 Recherchez le message d'erreur Point de terminaison associé introuvable.

Par exemple,

```
L'exception suivante a été interceptée : impossible de trouver le point de terminaison associé
'expected endpoint name'.
```

- 3 Modifiez votre point de terminaison vSphere pour qu'il corresponde au nom de point de terminaison attendu affiché dans le message du journal.
 - a Sélectionnez **Infrastructure > Points de terminaison > Points de terminaison**.
 - b Cliquez sur le nom du point de terminaison à modifier.
 - c Entrez le nom du point de terminaison dans la zone de texte **Nom**.
 - d Cliquez sur **OK**.

L'agent proxy peut échanger avec le point de terminaison et la collecte de données aboutit.

Créer un groupe Fabric

Vous pouvez organiser les ressources d'infrastructure en groupes Fabric et affecter un ou plusieurs administrateurs Fabric pour gérer les ressources du groupe Fabric.

Les groupes Fabric sont requis pour les points de terminaison virtuels et cloud. Vous pouvez attribuer un rôle d'administrateur Fabric à plusieurs utilisateurs en ajoutant plusieurs utilisateurs à la fois ou en choisissant un groupe de magasin d'identités ou un groupe personnalisé comme administrateur Fabric.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur laaS**.
- Créez au moins un point de terminaison. Reportez-vous à [Choisir un scénario de point de terminaison](#).

Procédure

- 1 Sélectionnez **Infrastructure > Groupes Fabric**.
- 2 Cliquez sur **Nouveau groupe Fabric**.
- 3 Entrez un nom dans la zone de texte **Nom**.
- 4 (Facultatif) Entrez une description dans la zone de texte **Description**.
- 5 Entrez un nom d'utilisateur ou un nom de groupe dans la zone de texte **Administrateurs Fabric** et appuyez sur Entrée.

Répétez cette étape pour ajouter plusieurs utilisateurs ou groupes au rôle.

- 6 Cliquez sur une ou plusieurs **ressources de calcul** à inclure dans votre groupe Fabric.

Seules les ressources qui existent sur les clusters que vous sélectionnez pour votre groupe Fabric sont découvertes lors de la collecte des données. Par exemple, seuls les modèles qui existent sur les clusters que vous sélectionnez sont découverts et disponibles pour le clonage sur les réservations que vous créez pour les groupes d'activité.

- 7 Cliquez sur **OK**.

Les administrateurs Fabric peuvent maintenant configurer des préfixes de machines. Reportez-vous à [Configurer des préfixes de machines](#).

Les utilisateurs connectés dans la console de vRealize Automation doivent se déconnecter et se reconnecter à la console de vRealize Automation pour pouvoir accéder aux pages pour lesquelles ils ont obtenu l'accès.

Configurer des préfixes de machines

Vous pouvez créer des préfixes de machine utilisés pour créer des noms de machines provisionnées via vRealize Automation. Un préfixe de machine est requis lors de la définition d'un composant de machine dans le canevas de conception du Blueprint.

Un préfixe est un nom de base suivi d'un compteur composé d'un nombre de chiffres spécifiés. Lorsque tous les chiffres sont utilisés, vRealize Automation revient au premier nombre.

Les préfixes de machine doivent respecter les limitations suivantes :

- Contenir uniquement des lettres ASCII ne respectant pas la casse a à z, les chiffres 0 à 9 et le trait d'union (-).
- Ne pas commencer par un trait d'union.
- Aucun autre symbole, caractère de ponctuation ou espace ne peut être utilisé.
- Longueur maximale de 15 caractères, y compris les chiffres, pour se conformer à la limite Windows de 15 caractères dans les noms d'hôtes.

Les noms d'hôtes plus longs sont tronqués lors du provisionnement d'une machine et mis à jour lors de la collecte de données suivante. Cependant, pour le provisionnement WIM, les noms ne sont pas tronqués et le provisionnement échoue lorsque le nom spécifié comporte plus de 15 caractères.

- vRealize Automation ne prend pas en charge plusieurs machines virtuelles portant le même nom dans une même instance. Si vous choisissez une convention de dénomination qui permet un chevauchement des noms de machines, vRealize Automation ne provisionne pas une machine portant le nom redondant. Si possible, vRealize Automation ignore le nom qui est déjà utilisé et génère un nouveau nom de machine en utilisant le préfixe de machine spécifié. Si un nom unique ne peut pas être généré, le provisionnement échoue.

Prérequis

Connectez-vous à la console de vRealize Automation en tant qu'**administrateur Fabric**.

Procédure

- 1 Cliquez sur **Infrastructure > Administration > Préfixes de machine**.
- 2 Cliquez sur **Nouveau**.
- 3 Entrez le préfixe de machine dans la zone de texte **Nom**.
- 4 Entrez le nombre de chiffres de compteur dans la zone de texte **Nombre de chiffres**.
- 5 Entrez le numéro de départ du compteur dans la zone de texte **Numéro suivant**.
- 6 Cliquez sur l'icône **Enregistrer** (✓).

Les administrateurs de locataires peuvent créer des groupes d'activité afin que les utilisateurs puissent accéder à vRealize Automation pour demander des machines.

Création d'un profil réseau

Un profil réseau contient des informations IP, telles que passerelle, sous-réseau et plage d'adresses. vRealize Automation utilise vSphere DHCP ou un fournisseur IPAM spécifié pour attribuer les adresses IP aux machines qu'il provisionne.

Vous pouvez créer un profil réseau pour définir un type de réseau disponible. Vous pouvez créer des profils réseau externes et des modèles de traduction d'adresses réseau (NAT) à la demande et des profils réseau acheminés qui créent les commutateurs logiques NSX et les paramètres de routage appropriés pour un nouveau chemin réseau. Des profils réseau sont requis lors de l'ajout de composants réseau à un Blueprint.

Les profils réseau sont utilisés pour configurer des paramètres réseaux lors du provisionnement de machines. Les profils réseau spécifient également la configuration de dispositifs NSX Edge qui sont créés lors du provisionnement de machines. Vous identifiez un profil réseau lorsque vous créez des réservations et des Blueprints. Dans une réservation, vous pouvez attribuer un profil réseau à un chemin réseau et spécifier un de ces chemins pour un composant de machine dans un Blueprint.

Un créateur de Blueprint spécifie un profil réseau approprié lors de la définition de composants réseau dans le Blueprint. Vous pouvez utiliser un profil réseau existant et un profil réseau NAT ou acheminé à la demande lorsque vous définissez les adaptateurs réseau et les équilibrages de charge pour la machine de provisionnement.

Les profils réseau prennent également en charge les fournisseurs de gestion d'adresses IP (IPAM) tiers, tels qu'Infoblox. Lorsque vous configurez un profil réseau pour IPAM, vos machines provisionnées peuvent obtenir leurs données d'adresses IP, ainsi que des informations associées, telles que serveur DNS et passerelle, à partir de la solution IPAM configurée. Vous pouvez utiliser un module IPAM externe pour un fournisseur tiers, tel qu'Infoblox, pour définir un point de terminaison IPAM à utiliser avec un profil réseau.

Remarque Si vous utilisez un fournisseur IPAM tiers et que vous souhaitez spécifier sur quel réseau déployer votre machine, utilisez un profil réseau distinct pour chaque VLAN afin d'éviter le problème connu décrit dans [l'article 2148656 de la base de connaissances](#).

Si vous n'utilisez pas de fournisseur IPAM tiers mais le point de terminaison IPAM fourni par vRealize Automation, vous pouvez spécifier les plages d'adresses IP que les profils réseau peuvent utiliser. Chaque adresse IP figurant dans les plages allouées à une machine est récupérée pour être réaffectée lorsque la machine est détruite. Vous pouvez créer un profil réseau pour définir une plage d'adresses IP statiques pouvant être attribuée aux machines. Lorsque le provisionnement de machines virtuelles s'effectue par clonage ou à l'aide de la méthode kickstart ou autoYaST, le propriétaire des machines demandeuses peut attribuer des adresses IP statiques à partir d'une plage prédéterminée.

Vous pouvez attribuer un profil réseau à un chemin réseau spécifique sur une réservation. Pour certains types de composants de machine, tels que vSphere, vous pouvez attribuer un profil réseau lorsque vous créez ou modifiez des Blueprints.

Remarque Vous ne pouvez pas modifier le profil réseau d'une machine virtuelle déployée, mais vous pouvez modifier le réseau auquel la machine virtuelle est connectée. Si le réseau est associé à un profil réseau différent, vRealize Automation attribue une adresse IP à partir de ce profil réseau à la machine virtuelle. La machine virtuelle continue cependant à utiliser l'ancienne adresse IP jusqu'à ce que vous mettiez à jour l'adresse IP sur le système d'exploitation invité. Vous pouvez éventuellement utiliser l'action de reconfiguration sur la machine virtuelle déployée, ce qui nécessite également de mettre à jour l'adresse IP sur le système d'exploitation invité.

Si vous spécifiez un profil réseau dans une réservation et un Blueprint, la valeur du Blueprint est prioritaire. Par exemple, si vous spécifiez un profil réseau dans le Blueprint à l'aide de la propriété personnalisée `VirtualMachine.NetworkN.ProfileName` et dans une réservation utilisée par le Blueprint, le profil réseau spécifié dans le Blueprint est prioritaire. Toutefois, si la propriété personnalisée n'est pas utilisée dans le Blueprint et que vous sélectionnez un profil réseau pour la carte réseau d'une machine, vRealize Automation utilise le chemin d'accès de réseau de réservation pour la carte réseau de la machine pour laquelle le profil réseau est spécifié.

Pour plus d'informations sur ces types de réseau, reportez-vous au *Guide d'Administration de NSX* dans le centre d'informations de NSX sur https://www.vmware.com/support/pubs/nsx_pubs.html.

Tableau 2-14. Types de réseau disponibles pour un profil réseau vRealize Automation

Type de réseau	Description
Externe	<p>Réseau existant configuré sur le serveur vSphere. Partie externe des types de réseaux NAT et acheminés. Un profil réseau externe peut définir une plage d'adresses IP statiques disponibles sur le réseau externe.</p> <p>Vous pouvez utiliser les plages d'adresses IP obtenues auprès du point de terminaison VMware IPAM fourni ou d'un point de terminaison d'un fournisseur de services IPAM tiers enregistré et configuré dans vRealize Orchestrator, par exemple, Infoblox IPAM. Un plage d'adresses IP est créée à partir d'un bloc d'IP lors de l'allocation.</p> <p>Un profil réseau externe avec une plage d'adresses IP statiques est un composant requis pour les réseaux NAT et acheminés.</p> <p>Reportez-vous à Création d'un profil réseau externe pour un réseau existant.</p>
NAT	<p>Réseau à la demande créé lors du provisionnement. Réseaux NAT qui utilisent un ensemble d'adresses IP pour la communication externe et un autre ensemble pour les communications internes.</p> <p>Avec les réseaux NAT Un à un, une adresse IP externe est attribuée à chaque machine virtuelle à partir du profil réseau externe, et une adresse IP interne est attribuée à partir du profil réseau NAT. Avec les réseaux NAT Un à plusieurs, toutes les machines partagent une adresse IP unique du profil réseau externe pour la communication externe.</p> <p>Vous pouvez utiliser les plages d'adresses IP obtenues auprès du point de terminaison VMware IPAM fourni ou d'un point de terminaison d'un fournisseur de services IPAM tiers enregistré et configuré dans vRealize Orchestrator, par exemple, Infoblox IPAM. Un plage d'adresses IP est créée à partir d'un bloc d'IP lors de l'allocation.</p> <p>Un profil réseau NAT définit des réseaux locaux et externes qui utilisent une table de traductions pour la communication mutuelle.</p> <p>Reportez-vous à Création d'un profil réseau NAT pour un réseau à la demande.</p>
Acheminé	<p>Réseau à la demande créé lors du provisionnement. Les réseaux acheminés contiennent un espace IP routable réparti entre des sous-réseaux qui sont reliés à l'aide d'un routeur logique distribué (DLR).</p> <p>Le sous-réseau disponible suivant est attribué à chaque nouveau réseau acheminé et est associé aux autres réseaux acheminés qui utilisent le même profil réseau. Les machines virtuelles provisionnées avec des réseaux acheminés qui ont le même profil réseau acheminé peuvent communiquer entre elles et avec le réseau externe.</p> <p>Vous pouvez utiliser les plages d'adresses IP obtenues auprès du point de terminaison VMware IPAM fourni ou d'un point de terminaison d'un fournisseur de services IPAM tiers enregistré et configuré dans vRealize Orchestrator, par exemple, Infoblox IPAM. Un plage d'adresses IP est créée à partir d'un bloc d'IP lors de l'allocation.</p> <p>Un profil réseau acheminé définit un espace routable et les sous-réseaux disponibles.</p> <p>Reportez-vous à Création d'un profil réseau acheminé pour un réseau à la demande.</p>

Utilisation de profils réseau pour contrôler les plages d'adresses IP

Vous pouvez utiliser des profils réseau pour attribuer des adresses IP statiques dans une plage prédéfinie à des machines virtuelles provisionnées par clonage à l'aide de kickstart Linux ou autoYaST, ou à des machines de cloud provisionnées dans OpenStack à l'aide de kickstart.

Par défaut, vRealize Automation utilise le protocole DHCP pour attribuer des adresses IP à des machines provisionnées.

Vous pouvez créer des profils réseau afin de définir une plage d'adresses IP statiques que vous pouvez attribuer à des machines. Vous pouvez attribuer des profils réseau à des chemins réseau spécifiques sur une réservation. Les machines provisionnées par clonage ou à l'aide de kickstart ou d'autoYaST et qui sont attachées à un chemin d'accès au réseau avec un profil réseau associé sont provisionnées avec une adresse IP statique attribuée. Pour réaliser un provisionnement à l'aide d'une attribution d'adresse IP statique, vous devez utiliser une spécification de personnalisation.

Vous pouvez attribuer un profil réseau à un composant de machine vSphere dans un Blueprint en ajoutant un réseau NAT à la demande existant ou un composant réseau acheminé à la demande au canevas de conception et en sélectionnant un profil réseau à connecter au composant de machine vSphere. Vous pouvez également attribuer des profils réseau à des Blueprints à l'aide de la propriété personnalisée `VirtualMachine.NetworkN.ProfileName`, dans laquelle *N* désigne l'identifiant du réseau.

Vous pouvez également utiliser le point de terminaison IPAM vRealize Automation fourni ou un point de terminaison de fournisseur de service IPAM tiers dans votre profil réseau pour obtenir et configurer les adresses IP. Pour plus d'informations sur la configuration requise du fournisseur IPAM externe, reportez-vous à [Liste de contrôle pour assurer la prise en charge d'un fournisseur IPAM tiers](#).

Lorsque vous sélectionnez un point de terminaison d'un fournisseur de services IPAM tiers dans un profil réseau, vRealize Automation récupère les plages d'adresses IP à partir du point de terminaison du fournisseur IPAM externe enregistré, par exemple Infoblox. Il attribue ensuite les valeurs IP à partir de ce point de terminaison. Le masque de sous-réseau de la plage spécifié est utilisé pour allouer des sous-réseaux à partir du bloc d'IP.

Si vous spécifiez un profil réseau dans une réservation et un Blueprint, la valeur du Blueprint est prioritaire. Par exemple, si vous spécifiez un profil réseau dans le Blueprint à l'aide de la propriété personnalisée `VirtualMachine.NetworkN.ProfileName` et dans une réservation utilisée par le Blueprint, le profil réseau spécifié dans le Blueprint est prioritaire. Toutefois, si la propriété personnalisée n'est pas utilisée dans le Blueprint et que vous sélectionnez un profil réseau pour la carte réseau d'une machine, vRealize Automation utilise le chemin d'accès de réseau de réservation pour la carte réseau de la machine pour laquelle le profil réseau est spécifié.

Présentation du format de fichier CSV pour importer des adresses IP de profil réseau

Vous pouvez importer des plages réseau d'adresses IP à un profil réseau vRealize Automation à l'aide d'un fichier CSV correctement formaté.

Les entrées du fichier CSV doivent être au format suivant.

Champ CSV	Description
<code>ip_address</code>	Adresse IP au format IPv4.
<code>machine_name</code>	Nom d'une machine gérée dans vRealize Automation. Si le champ est vide, aucun nom n'est fourni par défaut. Si le champ est vide, la valeur du champ <code>status</code> ne peut pas être Allouée.
<code>status</code>	Allouée ou Non allouée, sensible à la casse. Si le champ est vide, la valeur par défaut est Non allouée. Si l'état est Allouée, le champ <code>machine_name</code> ne peut pas être vide.
<code>NIC_offset</code>	Entier non négatif. Facultatif.

L'exemple de saisie suivant ne spécifie pas un décalage de carte réseau :

```
100.10.100.1,mymachine01,Allocated
```

Importer des adresses IP dans un profil réseau à partir d'un fichier CSV

Vous pouvez ajouter des adresses IP à une plage de profil réseau en important un fichier CSV correctement formaté. Vous pouvez également modifier les adresses de la plage du profil réseau en modifiant la plage dans vRealize Automation ou en important un fichier CSV modifié ou différent.

Vous pouvez ajouter ou modifier les adresses IP d'une plage de profil réseau en procédant à une importation à partir d'un fichier CSV ou en entrant les valeurs manuellement. Vous pouvez également autoriser un fournisseur IPAM tiers à fournir des adresses IP.

- Importez une plage initiale d'adresses IP dans un profil réseau vRealize Automation.
- Appliquez les valeurs importées pour créer la première plage réseau nommée dans le profil réseau.
- Supprimez une ou plusieurs adresses IP de la plage réseau vRealize Automation.
- Importez un fichier CSV modifié ou différent pour examiner comment les valeurs de la plage réseau sont modifiées.

Vous ne pouvez pas utiliser l'option **Importer depuis un fichier CSV** pour les profils réseau qui utilisent un point de terminaison IPAM tiers, car les adresses IP sont gérées par le fournisseur IPAM tiers, pas par vRealize Automation.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur Fabric**.
- Créez un fichier CSV contenant des adresses IP à importer dans une plage réseau. Reportez-vous à la section [Créer un profil de réseau externe au moyen d'un fournisseur IPAM tiers](#) et [Présentation du format de fichier CSV pour importer des adresses IP de profil réseau](#).

Procédure

- 1 Sélectionnez **Infrastructure > Réservations > Profils réseau**.
- 2 Cliquez sur **Nouveau**, puis sélectionnez un type de profil réseau dans le menu déroulant.
Pour cet exemple, sélectionnez *Externe*.
- 3 Entrez **Mon profil réseau avec CSV** dans la zone de texte **Nom**.
- 4 Entrez **Test d'adresses IP d'une plage réseau avec CSV** dans la zone de texte **Description**.
L'option d'importation de fichier CSV s'applique aux paramètres des pages des onglets **Plages réseau** et **Adresses IP**. Nous passerons rapidement sur les deux premiers onglets pour entrer les informations de base du profil réseau.
- 5 Facultativement, sélectionnez un point de terminaison IPAM configuré si vous en avez un disponible. Sinon, ignorez cette étape.

- 6 Entrez une valeur d'adresse IP appropriée dans les zones de texte **Masque de sous-réseau** et **Passerelle**.
- 7 Cliquez sur l'onglet **DNS**.
- 8 Entrez les informations applicables telles qu'un suffixe DNS et cliquez sur l'onglet **Plages réseau**.
L'option **Importer depuis un fichier CVS** est disponible lorsque vous cliquez sur l'onglet **Plages réseau**.
- 9 Cliquez sur **Nouveau** pour entrer un nouveau nom de plage réseau et une plage d'adresses IP manuellement, ou cliquez sur **Importer depuis un fichier CSV** pour importer les informations d'adresses IP à partir d'un fichier CSV correctement formaté.

- Cliquez sur **Nouveau**.

- a Entrez un nom de plage réseau.
- b Entrez une description de plage réseau.
- c Entrez l'adresse IP de début de la plage.
- d Entrez l'adresse IP de fin de la plage.

- Cliquez sur **Importer à partir d'un fichier CSV**.

- a Accédez au fichier CSV, sélectionnez-le ou faites-le glisser dans la boîte de dialogue **Importer depuis un fichier CSV**.

Une ligne dans le fichier CSV a le format *ip_address, machine_name, status, NIC offset*. Par exemple :

```
100.10.100.1,mymachine01,Allocated
```

Champ CSV	Description
ip_address	Adresse IP au format IPv4.
machine_name	Nom d'une machine gérée dans vRealize Automation. Si le champ est vide, aucun nom n'est fourni par défaut. Si le champ est vide, la valeur du champ status ne peut pas être Allouée.
status	Allouée ou Non allouée, sensible à la casse. Si le champ est vide, la valeur par défaut est Non allouée. Si l'état est Allouée, le champ machine_name ne peut pas être vide.
NIC_offset	Entier non négatif. Facultatif.

- b Cliquez sur **Appliquer**.

- 10 Cliquez sur **OK**.

La plage d'adresses IP s'affiche dans la liste Plages définies. Les adresses IP de la plage s'affichent dans la liste Adresses IP définies.

Les adresses IP téléchargées s'affichent sur la page **Adresses IP** lorsque vous cliquez sur **Appliquer** après l'enregistrement et la modification du profil réseau.

- 11 Cliquez sur l'onglet **Adresses IP** pour afficher les données d'adresses IP pour l'espace d'adressage de la plage spécifiée.

Si vous avez importé les informations d'adresses IP à partir d'un fichier CSV, le nom de la plage généré est *Importé depuis un fichier CSV*.

- 12 (Facultatif) Sélectionnez les informations d'adresse IP à partir du menu déroulant **Plage réseau** pour filtrer les entrées d'adresses IP.

Vous pouvez afficher des informations sur toutes les plages réseau définies, les plages réseau importées depuis un fichier CSV ou une plage réseau nommée. Les détails inclut notamment l'adresse IP de début, le nom de la machine, la date et l'horodatage de la dernière modification et l'état IP.

Suivant

Si vous réimportez des adresses IP à partir d'un fichier CSV, les adresses IP précédentes sont remplacées par les informations du fichier CSV importé.

Création d'un profil réseau externe pour un réseau existant

Vous pouvez créer des profils réseau externes afin de spécifier les paramètres de configuration des réseaux existants pour le provisionnement des machines et des dispositifs NSX Edge qui seront utilisés lors du provisionnement.

Vous pouvez utiliser le point de terminaison de fournisseur IPAM vRealize Automation fourni ou un point de terminaison de fournisseur IPAM tiers, tel qu'Infoblox, que vous avez enregistré dans vRealize Orchestrator.

Créer un profil réseau externe en utilisant le point de terminaison IPAM fourni

Vous pouvez créer un profil réseau externe afin de définir des propriétés de réseau et une plage d'adresses IP statiques qui seront utilisées lors du provisionnement des machines sur un réseau existant.

Vous pouvez définir une ou plusieurs plages réseau d'adresses IP statiques dans le profil réseau à utiliser pour provisionner un réseau. Si vous ne spécifiez aucune plage, vous pouvez utiliser un profil réseau en tant que stratégie de réservation de réseau pour sélectionner un chemin réseau de réservation pour une carte réseau de machines virtuelles (vNIC, Virtual Machine Network Card).

Pour plus d'informations sur la création d'un profil réseau externe et l'utilisation d'un point de terminaison de fournisseur IPAM externe, reportez-vous à [Créer un profil de réseau externe au moyen d'un fournisseur IPAM tiers](#).

Procédure

- 1 [Spécifier les informations de Profil réseau externe au moyen du point de terminaison IPAM fourni](#)

Un profil réseau externe identifie les propriétés et les paramètres réseau d'un réseau existant. Un profil réseau externe est une condition préalable pour les profils réseau NAT et acheminés.

- 2 [Object Missing](#)

Suivant

Vous pouvez attribuer un profil réseau à un chemin réseau dans une réservation ou un architecte de Blueprint peut spécifier le profil réseau dans un Blueprint. Vous pouvez utiliser le profil réseau externe lorsque vous créez un réseau NAT à la demande ou un profil de réseau acheminé.

Spécifier les informations de Profil réseau externe au moyen du point de terminaison IPAM fourni

Un profil réseau externe identifie les propriétés et les paramètres réseau d'un réseau existant. Un profil réseau externe est une condition préalable pour les profils réseau NAT et acheminés.

Pour plus d'informations sur la création d'un profil réseau externe en obtenant les informations d'adresses IPAM à partir d'un point de terminaison IPAM tiers enregistré, tel qu'Infoblox, reportez-vous à [Liste de contrôle pour assurer la prise en charge d'un fournisseur IPAM tiers](#) et [Créer un profil de réseau externe au moyen d'un fournisseur IPAM tiers](#). Utilisez la procédure suivante pour créer un profil réseau en utilisant le point de terminaison IPAM interne VMware.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur Fabric**.

Procédure

- 1 Sélectionnez **Infrastructure > Réservations > Profils réseau**.
- 2 Cliquez sur **Nouveau**, puis sélectionnez **Existant** ou **Externe** dans le menu déroulant.
- 3 Entrez un nom et, éventuellement, une description.
- 4 Acceptez la valeur par défaut de **Point de terminaison IPAM** pour le point de terminaison IPAM **vRealize Automation** fourni.

- 5 Entrez un masque de sous-réseau IP dans la zone de texte **Masque de sous-réseau**.

Le masque de sous-réseau spécifie la taille totale de l'espace d'adressage routable que vous souhaitez définir pour votre profil réseau.

Par exemple, entrez 255.255.0.0.

- 6 Entrez une adresse de passerelle Edge ou acheminée dans la zone de texte **Passerelle**.

Utilisez un format d'adresse IPv4 standard. Par exemple, entrez 10.10.110.1.

L'adresse IP de la passerelle définie dans le profil réseau est attribuée à la carte réseau pendant l'allocation. Si aucune valeur n'est attribuée dans la zone de texte **Passerelle** du profil réseau, vous devez utiliser la propriété personnalisée `VirtualMachine.Network0.Gateway` lors du provisionnement de la machine Edge.

- 7 Cliquez sur l'onglet **DNS**.

8 Entrez les valeurs DNS et WINS requises.

Les valeurs DNS sont utilisées pour l'enregistrement et la résolution des noms DNS. Les champs DNS et WINS sont facultatifs si vous utilisez un point de terminaison IPAM interne. Si vous utilisez un point de terminaison IPAM externe, les valeurs DNS et WINS sont fournies par le fournisseur IPAM tiers.

- a (Facultatif) Entrez une valeur de serveur **DNS principal**.
- b (Facultatif) Entrez une valeur de serveur **DNS secondaire**.
- c (Facultatif) Entrez une valeur **Suffixes DNS**.
- d (Facultatif) Entrez une valeur **Suffixes de recherche DNS**.
- e (Facultatif) Entrez une valeur de serveur **Serveur WINS préféré**.
- f (Facultatif) Entrez une valeur de serveur **Serveur WINS auxiliaire**.

Suivant

Vous pouvez configurer des plages d'adresses IP pour les adresses IP statiques. Reportez-vous à [Object Missing](#).

Object Missing

This object is not available in the repository.

Créer un profil de réseau externe au moyen d'un fournisseur IPAM tiers

Vous pouvez importer un fournisseur IPAM tiers et l'enregistrer dans vRealize Orchestrator pour obtenir les adresses IP depuis ce fournisseur tiers.

Vous pouvez créer un profil réseau externe qui utilise un point de terminaison de fournisseur de solutions IPAM tiers enregistré afin d'obtenir des paramètres de passerelle, de masque de sous-réseau et DHCP/WINS.

Vous pouvez définir une ou plusieurs plages réseau d'adresses IP statiques dans le profil réseau à utiliser pour provisionner un réseau. Si vous ne spécifiez aucune plage, vous pouvez utiliser un profil réseau en tant que stratégie de réservation de réseau pour sélectionner un chemin réseau de réservation pour une carte réseau de machines virtuelles (vNIC, Virtual Machine Network Card).

Pour plus d'informations sur la création d'un profil réseau externe sans utiliser un fournisseur IPAM ou en utilisant le point de terminaison de fournisseur IPAM interne fourni, reportez-vous à [Créer un profil réseau externe en utilisant le point de terminaison IPAM fourni](#).

Procédure

1 Spécifier les informations d'un profil réseau externe en utilisant un point de terminaison IPAM tiers

Un profil réseau externe identifie les propriétés et les paramètres réseau d'un réseau existant. Un profil réseau externe est une condition préalable pour les profils réseau NAT et acheminés. Si vous avez enregistré et configuré un point de terminaison IPAM dans vRealize Orchestrator, vous pouvez spécifier que les informations relatives aux adresses IP soient fournies par un fournisseur IPAM.

2 Configurer les plages IP du profil de réseau externe au moyen d'un point de terminaison IPAM tiers

Vous pouvez définir une ou plusieurs plages réseau d'adresses IP statiques dans le profil réseau à utiliser pour provisionner un réseau. Si vous ne spécifiez aucune plage, vous pouvez utiliser un profil réseau en tant que stratégie de réservation de réseau pour sélectionner un chemin réseau de réservation pour une carte réseau de machines virtuelles (vNIC, Virtual Machine Network Card).

Suivant

Vous pouvez attribuer un profil réseau à un chemin réseau dans une réservation ou un architecte de Blueprint peut spécifier le profil réseau dans un Blueprint. Vous pouvez utiliser le profil réseau externe lorsque vous créez un réseau NAT à la demande ou un profil de réseau acheminé.

Spécifier les informations d'un profil réseau externe en utilisant un point de terminaison IPAM tiers

Un profil réseau externe identifie les propriétés et les paramètres réseau d'un réseau existant. Un profil réseau externe est une condition préalable pour les profils réseau NAT et acheminés. Si vous avez enregistré et configuré un point de terminaison IPAM dans vRealize Orchestrator, vous pouvez spécifier que les informations relatives aux adresses IP soient fournies par un fournisseur IPAM.

Prérequis

- Vérifiez que vous avez importé et configuré un plug-in de fournisseur IPAM dans vRealize Orchestrator et que vous avez enregistré un type de point de terminaison de fournisseur IPAM dans vRealize Orchestrator. Dans cet exemple, le fournisseur de solution IPAM externe pris en charge est Infoblox. Reportez-vous à [Liste de contrôle pour assurer la prise en charge d'un fournisseur IPAM tiers](#).
- [Créer un point de terminaison de fournisseur IPAM tiers](#).
- Configurez vRealize Orchestrator Appliance avec le workflow du point de terminaison IPAM enregistré en tant qu'instance autonome d'Orchestrator dans le locataire global (administrateur@vsphere.local).
- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur Fabric**.

Procédure

- 1 Sélectionnez **Infrastructure > Réservations > Profils réseau**.
- 2 Cliquez sur **Nouveau**, puis sélectionnez **Existant** ou **Externe** dans le menu déroulant.
- 3 Entrez un nom et, éventuellement, une description.
- 4 Si vous avez configuré un ou plusieurs points de terminaison IPAM tiers, sélectionnez un point de terminaison IPAM tiers dans le menu déroulant **Point de terminaison IPAM**.

Lorsque vous sélectionnez un point de terminaison d'un fournisseur de services IPAM tiers que vous avez enregistré dans vRealize Orchestrator, les adresses IP sont obtenues du fournisseur de services IPAM spécifié. Les spécifications IP telles que les options de masque de sous-réseau et DNS/WINS ne sont pas disponibles, car leurs fonctions sont contrôlées par le point de terminaison IPAM tiers sélectionné.

Suivant

Vous pouvez maintenant définir les plages d'adresses IP du réseau pour terminer la définition du profil réseau.

Configurer les plages IP du profil de réseau externe au moyen d'un point de terminaison IPAM tiers

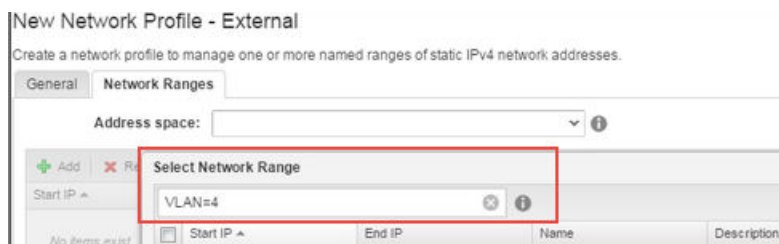
Vous pouvez définir une ou plusieurs plages réseau d'adresses IP statiques dans le profil réseau à utiliser pour provisionner un réseau. Si vous ne spécifiez aucune plage, vous pouvez utiliser un profil réseau en tant que stratégie de réservation de réseau pour sélectionner un chemin réseau de réservation pour une carte réseau de machines virtuelles (vNIC, Virtual Machine Network Card).

Vous pouvez définir des plages d'adresses IP en utilisant les adresses IP fournies par un fournisseur IPAM tiers.

vRealize Automation sauvegarde uniquement les ID de la plage IPAM externe dans la base de données et non les détails de la plage. Si vous modifiez un profil réseau sur cette page ou dans un Blueprint, vRealize Automation appelle le service IPAM pour obtenir les détails de la plage en fonction des ID de plage sélectionnés.

Remarque Il existe un problème connu chez certains fournisseurs IPAM tiers : une requête peut expirer lors du renvoi des plages réseau, entraînant l'obtention d'une liste vide. Pour résoudre ce problème, vous pouvez fournir des critères de recherche pour éviter l'expiration et obtenir les informations de la plage réseau.

Par exemple, en fonction de votre fournisseur IPAM, vous pouvez ajouter une propriété nommée VLAN à chaque réseau dans l'application du fournisseur IPAM et attribuer une valeur à cette propriété, par exemple 4. Vous pouvez ensuite filtrer par propriété et par valeur : par exemple VLAN=4, dans la zone de texte **Sélectionner une plage réseau** sur la page du profil réseau vRealize Automation.



Vous pouvez également augmenter le paramètre de délai d'expiration en procédant comme suit :

- 1 Sur chaque nœud du dispositif vRealize Automation, ouvrez le fichier `/etc/vcac/webapps/o11n-gateway-service/WEB-INF/classes/META-INF/spring/root/o11n-gateway-service-context.xml`.
- 2 Remplacez la valeur de délai d'expiration 30 secondes par une valeur plus élevée.
- 3 Redémarrez le serveur vcac en entrant `service vcac-server restart`.

Prérequis

[Spécifier les informations d'un profil réseau externe en utilisant un point de terminaison IPAM tiers.](#)

Procédure

- 1 Cliquez sur l'onglet **Plages réseau** pour créer une nouvelle plage réseau ou sélectionnez une plage réseau existante.

Les détails sur la plage sélectionnée s'affichent, incluant chaque nom, description, ainsi que les adresses IP de début et de fin. Des informations liées à l'état sont également fournies.

- 2 Sélectionnez un espace d'adressage dans la liste des espaces d'adressage disponibles pour le point de terminaison à partir du menu déroulant **Espace d'adressage**.

- 3 Cliquez sur **Ajouter** et sélectionnez une ou plusieurs plages réseau disponibles pour l'espace d'adressage en question.

La sélection d'une plage réseau peut produire une liste vide lorsque vous utilisez un fournisseur IPAM tiers. Pour plus d'informations, reportez-vous à l'article 2148656 de la base de connaissances à l'adresse <http://kb.vmware.com/kb/2148656>.

- 4 Cliquez sur **OK**.

La plage d'adresses IP s'affiche dans la liste Plages définies. Les adresses IP de la plage s'affichent dans la liste Adresses IP définies.

Les adresses IP téléchargées s'affichent sur la page **Adresses IP** lorsque vous cliquez sur **Appliquer** après l'enregistrement et la modification du profil réseau.

- 5 Cliquez sur **OK** pour terminer le profil réseau.

Suivant

Vous pouvez attribuer un profil réseau à un chemin réseau dans une réservation ou un architecte de Blueprint peut spécifier le profil réseau dans un Blueprint.

Création d'un profil réseau acheminé pour un réseau à la demande

Vous pouvez créer un profil réseau acheminé à la demande qui utilise le point de terminaison IPAM vRealize Automation fourni ou un point de terminaison IPAM tiers correctement configuré et enregistré.

Un profil réseau acheminé représente un espace IP routable qui est divisé entre plusieurs réseaux. Chaque nouveau réseau acheminé attribue le prochain sous-réseau disponible à partir de l'espace IP routable. Un réseau acheminé peut accéder à tous les autres réseaux acheminés qui utilisent le même profil réseau. Chaque sous-réseau acheminé peut accéder à tous les autres sous-réseaux créés par le même profil réseau.

Pour un fournisseur IPAM tiers, l'espace IP routable est créé et géré par le fournisseur IPAM tiers.

L'administrateur réseau utilise un fournisseur IPAM tiers pour définir un espace IP routable et créer un bloc d'adresses IP pour celui-ci. Vous pouvez sélectionner un ou plusieurs blocs d'adresses IP récupérés depuis le fournisseur IPAM tiers lorsque vous créez ou modifiez un profil réseau acheminé.

Lorsqu'une nouvelle instance d'un profil réseau acheminé est affectée depuis le fournisseur IPAM tiers, vRealize Automation appelle le fournisseur pour réserver le sous-réseau disponible suivant et crée une plage. Pour cela, elle utilise des blocs IP qui sont déterminés par le profil de réseau acheminé et la taille du sous-réseau. La plage résultante sert à affecter des adresses IP aux machines qui sont affectées au réseau acheminé dans le cadre du même déploiement.

Créer un profil réseau acheminé en utilisant le point de terminaison IPAM fourni

Lors de l'utilisation d'un profil réseau acheminé avec le point de terminaison IPAM fourni, vous pouvez définir un espace IP routable et les sous-réseaux disponibles pour un réseau acheminé à la demande.

En utilisant le point de terminaison IPAM vRealize Automation fourni, vous pouvez affecter des plages d'adresses IP statiques et une adresse IP de base au profil réseau acheminé.

Vous pouvez utiliser les plages d'adresses IP obtenues auprès du point de terminaison VMware IPAM fourni ou d'un point de terminaison d'un fournisseur de services IPAM tiers enregistré et configuré dans vRealize Orchestrator, par exemple, Infoblox IPAM. Un plage d'adresses IP est créée à partir d'un bloc d'IP lors de l'allocation.

Procédure

1 [Spécifier les informations du profil réseau acheminé avec le point de terminaison IPAM vRealize Automation](#)

Les informations du profil réseau identifient les propriétés du réseau acheminé, son profil réseau externe sous-jacent et les autres valeurs utilisées dans le provisionnement du réseau lorsque le point de terminaison IPAM fourni est utilisé.

2 [Configurer des plages d'adresses IP de réseau acheminé avec le point de terminaison IPAM vRealize Automation](#)

Vous pouvez définir une ou plusieurs plages d'adresses IP statiques à utiliser pour provisionner un réseau.

Spécifier les informations du profil réseau acheminé avec le point de terminaison IPAM vRealize Automation

Les informations du profil réseau identifient les propriétés du réseau acheminé, son profil réseau externe sous-jacent et les autres valeurs utilisées dans le provisionnement du réseau lorsque le point de terminaison IPAM fourni est utilisé.

Si vous souhaitez créer un profil réseau routé à l'aide d'un point de terminaison IPAM tiers, reportez-vous à la section [Spécifier les informations du profil réseau acheminé avec un point de terminaison IPAM tiers](#).

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur Fabric**.
- Créez un profil réseau externe. Reportez-vous à [Créer un profil réseau externe en utilisant le point de terminaison IPAM fourni](#).

Procédure

1 Sélectionnez **Infrastructure > Réservations > Profils réseau**.

- 2 Cliquez sur **Nouveau**, puis sélectionnez **Acheminé** dans le menu déroulant.
- 3 Entrez un nom et, éventuellement, une description.
- 4 Acceptez la valeur par défaut de **Point de terminaison IPAM** pour le point de terminaison IPAM **vRealize Automation** fourni.
- 5 Sélectionnez un profil réseau existant dans le menu déroulant **Profil réseau externe**.
- 6 Entrez le masque de sous-réseau dans la zone de texte **Masque de sous-réseau** qui est associée au profil réseau externe.

Le masque de sous-réseau spécifie la taille totale de l'espace d'adressage routable que vous souhaitez définir pour votre profil réseau.

Par exemple, entrez 255.255.0.0.

- 7 Sélectionnez une valeur dans la zone de texte **Masque de sous-réseau de la plage** pour déterminer combien de plages sont générées par l'option **Générer les plages** sur la page **Plages d'adresses IP**.

Par exemple, entrez 255.255.255.0.

Le masque de sous-réseau de la plage définit comment vous souhaitez partitionner cet espace en blocs d'adresses individuels alloués à chaque instance de déploiement de ce profil réseau. Lorsque vous sélectionnez une valeur pour le masque de sous-réseau de la plage, prenez en compte le nombre de déploiements que vous prévoyez d'utiliser pour le réseau acheminé.

Une plage est utilisée pour chaque déploiement utilisant un profil réseau acheminé. Le nombre de plages acheminées disponibles est égal au masque de sous-réseau divisé par le masque de sous-réseau de la plage, par exemple : $255.255.0.0/255.255.255.0 = 256$.

- 8 Entrez la première adresse IP disponible dans la zone de texte **Adresse IP de base**.

Cette option n'est pas disponible si vous sélectionnez un point de terminaison tiers.

Par exemple, entrez 120.120.0.1.

- 9 Cliquez sur l'onglet **DNS**.
- 10 Entrez les valeurs DNS et WINS requises.

Les valeurs DNS sont utilisées pour l'enregistrement et la résolution des noms DNS. Les champs DNS et WINS sont facultatifs si vous utilisez un point de terminaison IPAM interne. Si vous utilisez un point de terminaison IPAM externe, les valeurs DNS et WINS sont fournies par le fournisseur IPAM tiers.

- a (Facultatif) Entrez une valeur de serveur **DNS principal**.
- b (Facultatif) Entrez une valeur de serveur **DNS secondaire**.
- c (Facultatif) Entrez une valeur **Suffixes DNS**.
- d (Facultatif) Entrez une valeur **Suffixes de recherche DNS**.

- e (Facultatif) Entrez une valeur de serveur **Serveur WINS préféré**.
- f (Facultatif) Entrez une valeur de serveur **Serveur WINS auxiliaire**.

Suivant

[Configurer des plages d'adresses IP de réseau acheminé avec le point de terminaison IPAM vRealize Automation.](#)

Configurer des plages d'adresses IP de réseau acheminé avec le point de terminaison IPAM vRealize Automation

Vous pouvez définir une ou plusieurs plages d'adresses IP statiques à utiliser pour provisionner un réseau.

Lors du provisionnement, chaque nouveau réseau acheminé attribue la prochaine plage disponible et l'utilise comme son espace IP.

Prérequis

[Spécifier les informations du profil réseau acheminé avec le point de terminaison IPAM vRealize Automation.](#)

Procédure

- 1 Cliquez sur l'onglet **Plages réseau** pour créer une nouvelle plage réseau ou sélectionnez une plage réseau existante.

Les détails sur la plage sélectionnée s'affichent, incluant chaque nom, description, ainsi que les adresses IP de début et de fin. Des informations liées à l'état sont également fournies.

- 2 Cliquez sur **Générer les plages** pour générer des plages réseau basées sur le masque de sous-réseau, le masque de sous-réseau de la plage et les informations d'adresses IP de base que vous avez entrées dans l'onglet Général.

En commençant par les adresses IP de base, vRealize Automation génère les plages en fonction du masque de sous-réseau de la plage.

Par exemple, vRealize Automation génère des plages de 255 plages d'adresse IP si le masque de sous-réseau est 255.255.0.0 et le masque de sous-réseau de la plage est 255.255.255.0 en utilisant le nom Range1 à Rangen.

- 3 Cliquez sur **OK**.

Créer un profil de réseau acheminé au moyen d'un point de terminaison IPAM tiers

Lorsque vous utilisez un profil réseau acheminé avec un point de terminaison IPAM tiers, l'espace IP routable est créé et géré par le fournisseur IPAM tiers.

Lorsque vous utilisez un point de terminaison IPAM tiers dans le profil réseau acheminé, le fournisseur crée de nouvelles plages d'adresses IP pour chaque instance du réseau à la demande.

Vous pouvez utiliser les plages d'adresses IP obtenues auprès du point de terminaison VMware IPAM fourni ou d'un point de terminaison d'un fournisseur de services IPAM tiers enregistré et configuré dans vRealize Orchestrator, par exemple, Infoblox IPAM. Une plage d'adresses IP est créée à partir d'un bloc d'IP lors de l'allocation.

Procédure

1 Spécifier les informations du profil réseau acheminé avec un point de terminaison IPAM tiers

Les informations du profil réseau identifient les propriétés du réseau acheminé, son profil réseau externe sous-jacent et les autres valeurs utilisées dans le provisionnement du réseau lorsqu'un point de terminaison IPAM tiers est utilisé.

2 Configurer des plages d'adresses IP de réseau acheminé avec un point de terminaison IPAM tiers

Vous pouvez gérer une ou plusieurs plages nommées d'adresses réseau IPv4 à utiliser lors du provisionnement d'un réseau.

Spécifier les informations du profil réseau acheminé avec un point de terminaison IPAM tiers

Les informations du profil réseau identifient les propriétés du réseau acheminé, son profil réseau externe sous-jacent et les autres valeurs utilisées dans le provisionnement du réseau lorsqu'un point de terminaison IPAM tiers est utilisé.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur Fabric**.
- Créez un profil réseau externe. Reportez-vous à la section [Créer un profil réseau externe en utilisant le point de terminaison IPAM fourni](#) ou [Créer un profil de réseau externe au moyen d'un fournisseur IPAM tiers](#).
- Créez et configurez un point de terminaison IPAM tiers. Reportez-vous à [Créer un point de terminaison de fournisseur IPAM tiers](#).

Procédure

- 1 Sélectionnez **Infrastructure > Réservations > Profils réseau**.
- 2 Cliquez sur **Nouveau**, puis sélectionnez **Acheminé** dans le menu déroulant.
- 3 Entrez un nom et, éventuellement, une description.
- 4 Si vous avez configuré un ou plusieurs points de terminaison IPAM tiers, sélectionnez un point de terminaison IPAM tiers dans le menu déroulant **Point de terminaison IPAM**.

Lorsque vous sélectionnez un point de terminaison d'un fournisseur de services IPAM tiers que vous avez enregistré dans vRealize Orchestrator, les adresses IP sont obtenues du fournisseur de services IPAM spécifié. Les spécifications IP telles que les options de masque de sous-réseau et DNS/WINS ne sont pas disponibles, car leurs fonctions sont contrôlées par le point de terminaison IPAM tiers sélectionné.

- 5 Sélectionnez un profil réseau existant dans le menu déroulant **Profil réseau externe**.

Seuls les profils réseau configurés pour utiliser le point de terminaison IPAM sont répertoriés et disponibles pour être sélectionnés.

- 6 Sélectionnez une valeur dans le menu déroulant de la zone de texte **Masque de sous-réseau de la plage** pour déterminer le nombre de sous-réseaux créés pour le provisionnement.

Par exemple, entrez 255.255.255.0.

Le masque de sous-réseau de la plage définit comment vous souhaitez partitionner cet espace en blocs d'adresses individuels alloués à chaque instance de déploiement de ce profil réseau. Lorsque vous sélectionnez une valeur pour le masque de sous-réseau de la plage, prenez en compte le nombre de déploiements que vous prévoyez d'utiliser pour le réseau acheminé.

Une plage est utilisée pour chaque déploiement utilisant un profil réseau acheminé. Le nombre de plages acheminées disponibles est égal au masque de sous-réseau divisé par le masque de sous-réseau de la plage, par exemple : $255.255.0.0/255.255.255.0 = 256$.

- 7 Cliquez sur l'onglet **Blocs d'IP** pour définir un espace d'adresses et gérer une ou plusieurs plages d'adresses réseau IPv4 statiques nommées.

Les blocs d'IP disponibles sont la source des plages d'adresses IP créées ou allouées pour un acheminement à la demande.

Suivant

[Configurer des plages d'adresses IP de réseau acheminé avec un point de terminaison IPAM tiers.](#)

Configurer des plages d'adresses IP de réseau acheminé avec un point de terminaison IPAM tiers

Vous pouvez gérer une ou plusieurs plages nommées d'adresses réseau IPv4 à utiliser lors du provisionnement d'un réseau.

Lors du provisionnement, chaque nouveau réseau acheminé attribue la prochaine plage disponible et l'utilise comme son espace IP. Les blocs d'IP sont obtenus du fournisseur IPAM tiers. Lors du provisionnement, un réseau acheminé est attribué à partir du bloc avec un masque de sous-réseau qui correspond à celui de la plage fournie.

Prérequis

[Spécifier les informations du profil réseau acheminé avec un point de terminaison IPAM tiers.](#)

Procédure

- 1 Sélectionnez un espace d'adressage dans le menu déroulant **Espace d'adressage** pour limiter les blocs d'IP disponibles pour le provisionnement.

Une fois que vous avez ajouté un ou plusieurs blocs d'IP dans la section au-dessous de la zone de texte Espace d'adressage, vous ne pouvez plus sélectionner de valeur **Espace adressage**. Un profil réseau acheminé ne peut pas couvrir plusieurs espaces d'adressage.

- 2 Ajoutez un ou plusieurs blocs d'IP ou plages de fournisseur IPAM à l'aide de la syntaxe de recherche spécifique au fournisseur, ou sélectionnez-les dans le menu déroulant Rechercher.

Les blocs d'IP sont obtenus du fournisseur IPAM tiers.

La sélection d'une plage réseau peut produire une liste vide lorsque vous utilisez un fournisseur IPAM tiers. Pour plus d'informations, reportez-vous à l'article 2148656 de la base de connaissances à l'adresse <http://kb.vmware.com/kb/2148656>.

- a Cliquez sur **Ajouter**.
 - b Cliquez sur **Rechercher**.
 - c Entrez la syntaxe de recherche ou sélectionnez un ou plusieurs blocs d'IP dans le menu déroulant.
 - d Cliquez sur **OK**.
- 3 Cliquez sur **Appliquer**.
 - 4 Cliquez sur **OK**.

Création d'un profil réseau NAT pour un réseau à la demande

Vous pouvez créer un profil réseau NAT à la demande qui utilise le point de terminaison IPAM vRealize Automation fourni ou un point de terminaison IPAM tiers correctement configuré et enregistré.

Créer un profil réseau NAT en utilisant le point de terminaison IPAM fourni

Vous pouvez créer un profil réseau NAT NSX à la demande lié à un profil réseau externe. Lorsque vous utilisez le point de terminaison IPAM vRealize Automation fourni, vous pouvez attribuer des plages d'adresses IP et DHCP statiques au profil réseau NAT.

Les réseaux NAT utilisent un ensemble d'adresses IP pour la communication externe et un autre pour la communication interne. Les adresses IP externes sont affectées depuis un profil réseau externe, tandis que les adresses IP NAT internes sont définies par un profil réseau NAT. Lorsque vous provisionnez un nouveau réseau NAT, une nouvelle instance du profil réseau NAT est créée et utilisée pour affecter les adresses IP des machines.

Vous pouvez utiliser les plages d'adresses IP obtenues auprès du point de terminaison VMware IPAM fourni ou d'un point de terminaison d'un fournisseur de services IPAM tiers enregistré et configuré dans vRealize Orchestrator, par exemple, Infoblox IPAM. Une plage d'adresses IP est créée à partir d'un bloc d'IP lors de l'allocation.

Pour un réseau Un à plusieurs NAT, vous pouvez définir les règles NAT qui peuvent être configurées lors de l'ajout d'un composant réseau NAT au Blueprint et être modifiés lorsque vous modifiez le réseau NAT dans un déploiement.

Procédure

1 [Spécifier les informations du profil réseau NAT avec le point de terminaison IPAM vRealize Automation](#)

Le profil réseau identifie les propriétés du réseau NAT, son profil réseau externe sous-jacent, le type NAT et d'autres valeurs utilisées pour provisionner le réseau en utilisant le point de terminaison IPAM vRealize Automation intégré.

2 [Configurer des plages d'adresses IP de profil réseau NAT avec le point de terminaison IPAM vRealize Automation](#)

Vous pouvez définir une ou plusieurs plages d'adresses IP statiques à utiliser pour provisionner un réseau.

Spécifier les informations du profil réseau NAT avec le point de terminaison IPAM vRealize Automation

Le profil réseau identifie les propriétés du réseau NAT, son profil réseau externe sous-jacent, le type NAT et d'autres valeurs utilisées pour provisionner le réseau en utilisant le point de terminaison IPAM vRealize Automation intégré.

Si vous voulez créer un profil réseau NAT qui utilise un point de terminaison IPAM tiers, reportez-vous à la section [Spécifier les informations du profil réseau NAT avec un point de terminaison IPAM tiers](#).

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur Fabric**.
- Créez un profil réseau externe. Reportez-vous à [Créer un profil réseau externe en utilisant le point de terminaison IPAM fourni](#).

Procédure

- 1 Sélectionnez **Infrastructure > Réservations > Profils réseau**.
- 2 Cliquez sur **Nouveau**, puis sélectionnez **NAT** dans le menu déroulant.
- 3 Entrez un nom et, éventuellement, une description.
- 4 Acceptez la valeur par défaut de **Point de terminaison IPAM** pour le point de terminaison IPAM **vRealize Automation** fourni.
- 5 Sélectionnez un profil réseau existant dans le menu déroulant **Profil réseau externe**.

- 6 Sélectionnez un type de traduction d'adresses réseau Un à un ou Un à plusieurs dans le menu déroulant **Type de NAT**.

Option	Description
Un à un	<p>Permet d'attribuer une adresse IP statique externe à chaque adaptateur réseau. Chaque machine peut accéder au réseau externe et est accessible depuis le réseau externe.</p> <p>Toutes les adresses IP externes qui sont attribuées à une liaison montante edge NSX doivent faire partie du même sous-réseau. Lorsque vous utilisez NAT 1:1 dans vRealize Automation, le profil réseau externe correspondant doit contenir uniquement des plages IP qui existent au sein d'un sous-réseau unique.</p>
Un à plusieurs	<p>Une adresse IP externe est partagée entre toutes les machines du réseau. Une machine interne peut avoir des adresses DHCP ou des adresses IP statiques. Chaque machine peut accéder au réseau externe, mais aucune machine n'est accessible depuis le réseau externe. Si vous sélectionnez cette option, cela permet de cocher la case Activé du groupe DHCP.</p> <p>Le type de traduction NAT Un à plusieurs vous permet de définir des règles NAT lorsque vous ajoutez un composant réseau NAT à un Blueprint.</p>

- 7 Entrez un masque de sous-réseau IP dans la zone de texte **Masque de sous-réseau**.

Le masque de sous-réseau spécifie la taille totale de l'espace d'adressage routable que vous souhaitez définir pour votre profil réseau.

Par exemple, entrez 255.255.0.0.

- 8 Entrez une adresse de passerelle Edge ou acheminée dans la zone de texte **Passerelle**.

Utilisez un format d'adresse IPv4 standard. Par exemple, entrez 10.10.110.1.

L'adresse IP de la passerelle définie dans le profil réseau est attribuée à la carte réseau pendant l'allocation. Si aucune valeur n'est attribuée dans la zone de texte **Passerelle** du profil réseau, vous devez utiliser la propriété personnalisée `VirtualMachine.Network0.Gateway` lors du provisionnement de la machine Edge.

- 9 (Facultatif) Dans le groupe DHCP, cochez la case **Activé** et entrez les valeurs **Début de la plage d'adresses IP** et **Fin de la plage d'adresses IP**.

Vous pouvez cocher la case uniquement si vous définissez le type de NAT sur Un à plusieurs.

- 10 (Facultatif) Configurez une durée de bail DHCP pour définir la période pendant laquelle une machine peut utiliser une adresse IP.

- 11 Cliquez sur l'onglet **DNS**.

12 Entrez les valeurs DNS et WINS requises.

Les valeurs DNS sont utilisées pour l'enregistrement et la résolution des noms DNS. Les champs DNS et WINS sont facultatifs si vous utilisez un point de terminaison IPAM interne. Si vous utilisez un point de terminaison IPAM externe, les valeurs DNS et WINS sont fournies par le fournisseur IPAM tiers.

- a (Facultatif) Entrez une valeur de serveur **DNS principal**.
- b (Facultatif) Entrez une valeur de serveur **DNS secondaire**.
- c (Facultatif) Entrez une valeur **Suffixes DNS**.
- d (Facultatif) Entrez une valeur **Suffixes de recherche DNS**.
- e (Facultatif) Entrez une valeur de serveur **Serveur WINS préféré**.
- f (Facultatif) Entrez une valeur de serveur **Serveur WINS auxiliaire**.

Suivant

[Configurer des plages d'adresses IP de profil réseau NAT avec le point de terminaison IPAM vRealize Automation.](#)

Configurer des plages d'adresses IP de profil réseau NAT avec le point de terminaison IPAM vRealize Automation

Vous pouvez définir une ou plusieurs plages d'adresses IP statiques à utiliser pour provisionner un réseau.

Vous ne pouvez pas créer de chevauchement entre les adresses IP de la plage réseau de début et de fin et les adresses DHCP. Si vous tentez d'enregistrer un profil qui contient des plages d'adresses qui se chevauchent, vRealize Automation affiche une erreur de validation.

Prérequis

[Spécifier les informations du profil réseau NAT avec le point de terminaison IPAM vRealize Automation.](#)

Procédure

- 1 Cliquez sur l'onglet **Plages réseau** pour créer une nouvelle plage réseau ou sélectionnez une plage réseau existante.

Les détails sur la plage sélectionnée s'affichent, incluant chaque nom, description, ainsi que les adresses IP de début et de fin. Des informations liées à l'état sont également fournies.
- 2 Cliquez sur **Nouveau** pour entrer un nouveau nom de plage réseau et une plage d'adresses IP manuellement, ou cliquez sur **Importer depuis un fichier CSV** pour importer les informations d'adresses IP à partir d'un fichier CSV correctement formaté.
 - Cliquez sur **Nouveau**.
 - a Entrez un nom de plage réseau.
 - b Entrez une description de plage réseau.
 - c Entrez l'adresse IP de début de la plage.

d Entrez l'adresse IP de fin de la plage.

■ Cliquez sur **Importer à partir d'un fichier CSV**.

- a Accédez au fichier CSV, sélectionnez-le ou faites-le glisser dans la boîte de dialogue **Importer depuis un fichier CSV**.

Une ligne dans le fichier CSV a le format *ip_address, machine_name, status, NIC offset*. Par exemple :

```
100.10.100.1,mymachine01,Allocated
```

Champ CSV	Description
ip_address	Adresse IP au format IPv4.
machine_name	Nom d'une machine gérée dans vRealize Automation. Si le champ est vide, aucun nom n'est fourni par défaut. Si le champ est vide, la valeur du champ status ne peut pas être Allouée.
status	Allouée ou Non allouée, sensible à la casse. Si le champ est vide, la valeur par défaut est Non allouée. Si l'état est Allouée, le champ machine_name ne peut pas être vide.
NIC_offset	Entier non négatif. Facultatif.

- b Cliquez sur **Appliquer**.

3 Cliquez sur **OK**.

La plage d'adresses IP s'affiche dans la liste Plages définies. Les adresses IP de la plage s'affichent dans la liste Adresses IP définies.

Les adresses IP téléchargées s'affichent sur la page **Adresses IP** lorsque vous cliquez sur **Appliquer** après l'enregistrement et la modification du profil réseau.

4 Cliquez sur l'onglet **Adresses IP** pour afficher les adresses IP de la plage réseau nommée.

5 (Facultatif) Sélectionnez les informations d'adresse IP à partir du menu déroulant **Plage réseau** pour filtrer les entrées d'adresses IP.

Vous pouvez afficher des informations sur toutes les plages réseau définies, les plages réseau importées depuis un fichier CSV ou une plage réseau nommée. Les détails inclut notamment l'adresse IP de début, le nom de la machine, la date et l'horodatage de la dernière modification et l'état IP.

6 (Facultatif) Sélectionnez un type de statut dans le menu déroulant **Statut IP** pour filtrer les entrées d'adresses IP uniquement à celle correspondant au statut IP sélectionné. Les paramètres Statut sont Allouée, Non allouée, Détruite et Expirée.

Pour les adresses IP qui sont dans un état Expirée ou Détruite, vous pouvez cliquer sur **Récupération** pour rendre ces plages d'adresses IP disponibles pour allocation. Vous devez enregistrer le profil pour appliquer la récupération. Comme les adresses ne sont pas récupérées immédiatement, la colonne de statut ne change pas immédiatement du statut Expirée ou Détruite à Allouée.

7 Cliquez sur **OK**.

Créer un profil de réseau NAT au moyen d'un point de terminaison IPAM tiers

Vous pouvez créer un profil réseau NAT NSX à la demande lié à un profil réseau externe. Lors de l'utilisation d'un profil réseau NAT NSX avec un point de terminaison IPAM tiers, l'espace IP est créé et géré par le fournisseur IPAM tiers.

Lorsque vous utilisez un point de terminaison IPAM tiers dans le profil réseau NAT, le fournisseur crée de nouvelles plages d'adresses IP pour chaque instance du réseau à la demande. Un ensemble interne d'adresses IP défini avec une ou plusieurs plages est créé dans le point de terminaison de fournisseur IPAM tiers pour chaque instance du réseau NAT. Ces plages IP servent à affecter des adresses IP aux machines affectées au réseau NAT dans le cadre du même déploiement. Dans la mesure où il ne peut pas y avoir d'adresses IP dupliquées au sein d'un espace d'adressage unique, un nouvel espace d'adressage est créé par le fournisseur pour chaque instance du réseau NAT. Lorsqu'un réseau NAT est détruit, ses plages sont détruites dans le point de terminaison du fournisseur de services IPAM et dans le nouvel espace d'adressage.

Vous pouvez utiliser les plages d'adresses IP obtenues auprès du point de terminaison VMware IPAM fourni ou d'un point de terminaison d'un fournisseur de services IPAM tiers enregistré et configuré dans vRealize Orchestrator, par exemple, Infoblox IPAM. Une plage d'adresses IP est créée à partir d'un bloc d'IP lors de l'allocation.

Pour un réseau Un à plusieurs NAT, vous pouvez définir les règles NAT qui peuvent être configurées lors de l'ajout d'un composant réseau NAT au Blueprint et être modifiés lorsque vous modifiez le réseau NAT dans un déploiement.

Procédure

1 Spécifier les informations du profil réseau NAT avec un point de terminaison IPAM tiers

Les informations du profil réseau identifient les propriétés du réseau NAT, son profil réseau externe sous-jacent et les autres valeurs utilisées dans le provisionnement du réseau lorsqu'un point de terminaison IPAM tiers est utilisé.

2 Configurer des plages d'adresses IP NAT avec un point de terminaison IPAM tiers

Vous pouvez définir une ou plusieurs plages d'adresses IP pour le provisionnement d'un réseau à l'aide de NAT.

Spécifier les informations du profil réseau NAT avec un point de terminaison IPAM tiers

Les informations du profil réseau identifient les propriétés du réseau NAT, son profil réseau externe sous-jacent et les autres valeurs utilisées dans le provisionnement du réseau lorsqu'un point de terminaison IPAM tiers est utilisé.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur Fabric**.
- Créez un profil réseau externe. Reportez-vous à la section [Créer un profil réseau externe en utilisant le point de terminaison IPAM fourni](#) ou [Créer un profil de réseau externe au moyen d'un fournisseur IPAM tiers](#).

- Créez et configurez un point de terminaison IPAM tiers. Reportez-vous à [Créer un point de terminaison de fournisseur IPAM tiers](#).

Procédure

- 1 Sélectionnez **Infrastructure > Réservations > Profils réseau**.
- 2 Cliquez sur **Nouveau**, puis sélectionnez **NAT** dans le menu déroulant.
- 3 Entrez un nom et, éventuellement, une description.
- 4 Si vous avez configuré un ou plusieurs points de terminaison IPAM tiers, sélectionnez un point de terminaison IPAM tiers dans le menu déroulant **Point de terminaison IPAM**.

Lorsque vous sélectionnez un point de terminaison d'un fournisseur de services IPAM tiers que vous avez enregistré dans vRealize Orchestrator, les adresses IP sont obtenues du fournisseur de services IPAM spécifié. Les spécifications IP telles que les options de masque de sous-réseau et DNS/WINS ne sont pas disponibles, car leurs fonctions sont contrôlées par le point de terminaison IPAM tiers sélectionné.

- 5 Sélectionnez un profil réseau existant dans le menu déroulant **Profil réseau externe**.
Seuls les profils réseau configurés pour utiliser le point de terminaison IPAM sont répertoriés et disponibles pour être sélectionnés.
- 6 Sélectionnez un type de traduction d'adresses réseau Un à un ou Un à plusieurs dans le menu déroulant **Type de NAT**.

Option	Description
Un à un	<p>Permet d'attribuer une adresse IP statique externe à chaque adaptateur réseau. Chaque machine peut accéder au réseau externe et est accessible depuis le réseau externe.</p> <p>Toutes les adresses IP externes qui sont attribuées à une liaison montante edge NSX doivent faire partie du même sous-réseau. Lorsque vous utilisez NAT 1:1 dans vRealize Automation, le profil réseau externe correspondant doit contenir uniquement des plages IP qui existent au sein d'un sous-réseau unique.</p>
Un à plusieurs	<p>Une adresse IP externe est partagée entre toutes les machines du réseau. Une machine interne peut utiliser uniquement des adresses IP statiques. Chaque machine peut accéder au réseau externe, mais aucune machine n'est accessible depuis le réseau externe.</p> <p>DHCP n'est pas pris en charge lors de l'utilisation du NAT avec un fournisseur IPAM tiers.</p> <p>Le type de traduction NAT Un à plusieurs vous permet de définir des règles NAT lorsque vous ajoutez un composant réseau NAT à un Blueprint.</p>

- 7 Entrez un masque de sous-réseau IP dans la zone de texte **Masque de sous-réseau**.

Le masque de sous-réseau spécifie la taille totale de l'espace d'adressage routable que vous souhaitez définir pour votre profil réseau.

Par exemple, entrez 255.255.0.0.

- 8 Entrez une adresse de passerelle Edge ou acheminée dans la zone de texte **Passerelle**.

Utilisez un format d'adresse IPv4 standard. Par exemple, entrez 10.10.110.1.

L'adresse IP de la passerelle définie dans le profil réseau est attribuée à la carte réseau pendant l'allocation. Si aucune valeur n'est attribuée dans la zone de texte **Passerelle** du profil réseau, vous devez utiliser la propriété personnalisée `VirtualMachine.Network0.Gateway` lors du provisionnement de la machine Edge.

- 9 Cliquez sur l'onglet **DNS**.

- 10 Entrez les valeurs DNS et WINS requises.

Les valeurs DNS sont utilisées pour l'enregistrement et la résolution des noms DNS. Les champs DNS et WINS sont facultatifs si vous utilisez un point de terminaison IPAM interne. Si vous utilisez un point de terminaison IPAM externe, les valeurs DNS et WINS sont fournies par le fournisseur IPAM tiers.

- a (Facultatif) Entrez une valeur de serveur **DNS principal**.
- b (Facultatif) Entrez une valeur de serveur **DNS secondaire**.
- c (Facultatif) Entrez une valeur **Suffixes DNS**.
- d (Facultatif) Entrez une valeur **Suffixes de recherche DNS**.
- e (Facultatif) Entrez une valeur de serveur **Serveur WINS préféré**.
- f (Facultatif) Entrez une valeur de serveur **Serveur WINS auxiliaire**.

Suivant

[Configurer des plages d'adresses IP NAT avec un point de terminaison IPAM tiers.](#)

Configurer des plages d'adresses IP NAT avec un point de terminaison IPAM tiers

Vous pouvez définir une ou plusieurs plages d'adresses IP pour le provisionnement d'un réseau à l'aide de NAT.

Prérequis

[Spécifier les informations du profil réseau NAT avec un point de terminaison IPAM tiers.](#)

Procédure

- 1 Cliquez sur l'onglet **Plages réseau** pour créer une nouvelle plage réseau ou sélectionnez une plage réseau existante.

Les détails sur la plage sélectionnée s'affichent, incluant chaque nom, description, ainsi que les adresses IP de début et de fin. Des informations liées à l'état sont également fournies.

- 2 Cliquez sur **Nouveau** pour entrer un nouveau nom de plage réseau et une plage d'adresses IP manuellement, ou cliquez sur **Importer depuis un fichier CSV** pour importer les informations d'adresses IP à partir d'un fichier CSV correctement formaté.

■ Cliquez sur **Nouveau**.

- a Entrez un nom de plage réseau.
- b Entrez une description de plage réseau.
- c Entrez l'adresse IP de début de la plage.
- d Entrez l'adresse IP de fin de la plage.

■ Cliquez sur **Importer à partir d'un fichier CSV**.

- a Accédez au fichier CSV, sélectionnez-le ou faites-le glisser dans la boîte de dialogue **Importer depuis un fichier CSV**.

Une ligne dans le fichier CSV a le format *ip_address, machine_name, status, NIC offset*. Par exemple :

```
100.10.100.1,mymachine01,Allocated
```

Champ CSV	Description
ip_address	Adresse IP au format IPv4.
machine_name	Nom d'une machine gérée dans vRealize Automation. Si le champ est vide, aucun nom n'est fourni par défaut. Si le champ est vide, la valeur du champ status ne peut pas être Allouée.
status	Allouée ou Non allouée, sensible à la casse. Si le champ est vide, la valeur par défaut est Non allouée. Si l'état est Allouée, le champ machine_name ne peut pas être vide.
NIC_offset	Entier non négatif. Facultatif.

- b Cliquez sur **Appliquer**.

- 3 Cliquez sur **OK**.

La plage d'adresses IP s'affiche dans la liste Plages définies. Les adresses IP de la plage s'affichent dans la liste Adresses IP définies.

Les adresses IP téléchargées s'affichent sur la page **Adresses IP** lorsque vous cliquez sur **Appliquer** après l'enregistrement et la modification du profil réseau.

- 4 Cliquez sur l'onglet **Adresses IP** pour afficher les adresses IP de la plage réseau nommée.

- 5 (Facultatif) Sélectionnez les informations d'adresse IP à partir du menu déroulant **Plage réseau** pour filtrer les entrées d'adresses IP.

Vous pouvez afficher des informations sur toutes les plages réseau définies, les plages réseau importées depuis un fichier CSV ou une plage réseau nommée. Les détails inclut notamment l'adresse IP de début, le nom de la machine, la date et l'horodatage de la dernière modification et l'état IP.

- 6 (Facultatif) Sélectionnez un type de statut dans le menu déroulant **Statut IP** pour filtrer les entrées d'adresses IP uniquement à celle correspondant au statut IP sélectionné. Les paramètres Statut sont Allouée, Non allouée, Détruite et Expirée.

Pour les adresses IP qui sont dans un état Expirée ou Détruite, vous pouvez cliquer sur **Récupération** pour rendre ces plages d'adresses IP disponibles pour allocation. Vous devez enregistrer le profil pour appliquer la récupération. Comme les adresses ne sont pas récupérées immédiatement, la colonne de statut ne change pas immédiatement du statut Expirée ou Détruite à Allouée.

- 7 Cliquez sur **OK**.

Libération des adresses IP en détruisant les machines provisionnées

Lorsque vous détruisez un déploiement, ses adresses IP sont supprimées. Les adresses IP allouées, par exemple les adresses IP dans une plage de profil réseau, sont libérées et mises à disposition pour le provisionnement suivant.

Lorsque vous détruisez une machine dotée d'une adresse IP statique, son adresse IP est de nouveau disponible pour être utilisée par d'autres machines. Il est possible que les adresses non utilisées ne soient pas disponibles immédiatement, car le processus de récupération des adresses IP statiques est exécuté toutes les 30 minutes.

Si vous utilisez un fournisseur IPAM tiers, vRealize Automation supprime les adresses IP associées en utilisant le workflow vRealize Orchestrator dans le plug-in ou module du fournisseur IPAM tiers.

Configuration de réservations et de stratégies de réservation

Une réservation vRealize Automation peut définir des stratégies, des priorités et des quotas qui déterminent le placement d'une machine pour des demandes de provisionnement.

Les stratégies de réservation restreignent le provisionnement d'une machine à un sous-ensemble des réservations disponibles. Les stratégies de réservation de stockage permettent aux architectes de Blueprints d'attribuer des volumes de machine à différentes banques de données.

Pour réussir le provisionnement, la réservation doit disposer de suffisamment de stockage. La disponibilité de stockage de la réservation dépend des conditions suivantes :

- Quantité de stockage disponible sur la banque de données/cluster.
- Quantité de stockage réservée pour cette banque de données/cluster.
- Quantité de stockage déjà allouée dans vRealize Automation

Par exemple, même si l'instance de vCenter Server dispose de stockage pour la banque de données/cluster, si un stockage suffisant n'est pas réservé dans la réservation, le provisionnement échoue avec l'erreur « Aucune réservation n'est disponible pour l'allocation... ». Le stockage alloué sur une réservation dépend du nombre de machines virtuelles (quel que soit leur état) sur cette réservation spécifique. Consultez l'article de la base de connaissances VMware *Machine XXX : Aucune réservation n'est disponible à allouer au sein du groupe XXX. Un stockage total de XX Go a été demandé (2151030)* à l'adresse <http://kb.vmware.com/kb/2151030> pour plus d'informations.

Réservations

Vous pouvez créer une réservation vRealize Automation afin d'allouer des ressources de provisionnement du groupe Fabric à un groupe d'activité spécifique.

Par exemple, vous pouvez utiliser des réservations pour spécifier qu'un partage de la mémoire, du CPU, de la mise en réseau et des ressources de stockage d'une ressource de calcul unique appartient à un groupe d'activité spécifique ou que certaines machines sont allouées à un groupe d'activité spécifique.

Remarque Le stockage et la mémoire alloués à une machine provisionnée via une réservation sont libérés lorsque la machine est supprimée dans vRealize Automation par l'action Détruire. Le stockage et la mémoire ne sont pas libérés si la machine est supprimée dans vCenter Server.

Vous pouvez créer une réservation pour les types de machine suivants :

- vSphere
- vCloud Air
- vCloud Director
- Amazon EC2
- Azure
- Hyper V (SCVMM)
- Hyper-V autonome
- KVM (RHEV)
- OpenStack
- XenServer

Vous pouvez configurer des paramètres de sécurité pour les machines virtuelles à provisionner en spécifiant des informations dans un script de réservation, de Blueprint ou d'agent invité. Si les machines à provisionner nécessitent un agent invité, vous devez ajouter une règle de sécurité contenant cette exigence à la réservation ou au Blueprint. Par exemple, si vous utilisez une stratégie de sécurité par défaut qui refuse la communication entre toutes les machines, et vous fiez-vous à une stratégie de sécurité distincte qui autorise la communication entre des machines spécifiques, l'agent invité doit être en mesure de communiquer avec vRealize Automation pendant la phase de personnalisation. Pour éviter ce problème lors du provisionnement des machines, utilisez une stratégie de sécurité par défaut qui autorise la communication pendant la phase de personnalisation.

Choisir un scénario de réservation

Vous pouvez créer des réservations afin d'attribuer des ressources aux groupes d'activité. En fonction de votre scénario, la procédure permettant de créer une réservation diffère.

Choisissez un scénario de réservation basé sur le type de point de terminaison cible.

Chaque groupe d'activité doit avoir au moins une réservation pour ses membres afin de provisionner des machines de ce type. Par exemple, un groupe d'activité avec une réservation OpenStack mais aucune réservation Amazon ne peut pas demander une machine à partir d'Amazon. Dans cet exemple, une réservation allouée spécifiquement pour les ressources Amazon doit être attribuée au groupe d'activité.

Tableau 2-15. Choisir un scénario de réservation

Scénario	Procédure
Créez une réservation vSphere.	Créer une réservation pour Hyper-V, KVM, SCVMM, vSphere ou XenServer
Créez une réservation afin d'attribuer des ressources pour un point de terminaison vCloud Air.	Créer une réservation vCloud Air
Créez une réservation afin d'attribuer des ressources pour un point de terminaison vCloud Director.	Créer une réservation vCloud Director
Créez une réservation afin d'attribuer des ressources sur une ressource Amazon (en utilisant ou sans utiliser Amazon Virtual Private Cloud).	Créer une réservation Amazon EC2
Créez une réservation afin d'attribuer des ressources sur une ressource OpenStack	Créer une réservation OpenStack
Créez une réservation afin d'attribuer des ressources pour Hyper-V.	Créer une réservation pour Hyper-V, KVM, SCVMM, vSphere ou XenServer
Créez une réservation afin d'attribuer des ressources pour KVM.	Créer une réservation pour Hyper-V, KVM, SCVMM, vSphere ou XenServer
Créez une réservation afin d'attribuer des ressources sur une ressource OpenStack .	Créer une réservation OpenStack
Créez une réservation afin d'attribuer des ressources pour SCVMM.	Créer une réservation pour Hyper-V, KVM, SCVMM, vSphere ou XenServer
Créez une réservation afin d'attribuer des ressources pour XenServer.	Créer une réservation pour Hyper-V, KVM, SCVMM, vSphere ou XenServer
Créez une réservation afin d'attribuer des ressources pour Microsoft Azure.	Créer une réservation pour Microsoft Azure

Création de réservations de catégories cloud

Une réservation de type de catégorie cloud fournit un accès aux services de provisionnement d'un compte de service cloud pour un groupe d'activité vRealize Automation particulier. Les types de réservation cloud disponibles incluent notamment Amazon, OpenStack, vCloud Air et vCloud Director.

Une réservation est un partage de la mémoire, du CPU, de la mise en réseau et des ressources de stockage d'une ressource de calcul allouée à un groupe d'activité vRealize Automation particulier.

Un groupe d'activité peut avoir plusieurs réservations sur un point de terminaison ou des réservations sur plusieurs points de terminaison.

Le modèle d'allocation pour une réservation dépend du modèle d'allocation du centre de données associé. Les modèles d'allocation disponibles sont le pool d'allocation, le paiement à l'utilisation et le pool de réservation. Pour plus d'informations sur les modèles d'allocation, reportez-vous à la documentation de vCloud Director ou de vCloud Air.

En plus de définir le partage des ressources Fabric attribuées au groupe d'activité, une réservation peut définir des stratégies, des priorités et des quotas qui déterminent le placement de la machine.

Pour réussir le provisionnement, la réservation doit disposer de suffisamment de stockage. La disponibilité de stockage de la réservation dépend des conditions suivantes :

- Quantité de stockage disponible sur la banque de données/cluster.
- Quantité de stockage réservée pour cette banque de données/cluster.
- Quantité de stockage déjà allouée dans vRealize Automation

Par exemple, même si l'instance de vCenter Server dispose de stockage pour la banque de données/cluster, si un stockage suffisant n'est pas réservé dans la réservation, le provisionnement échoue avec l'erreur « Aucune réservation n'est disponible pour l'allocation... ». Le stockage alloué sur une réservation dépend du nombre de machines virtuelles (quel que soit leur état) sur cette réservation spécifique. Consultez l'article de la base de connaissances VMware *Machine XXX : Aucune réservation n'est disponible à allouer au sein du groupe XXX. Un stockage total de XX Go a été demandé (2151030)* à l'adresse <http://kb.vmware.com/kb/2151030> pour plus d'informations.

Présentation de la logique de sélection pour les réservations de cloud

Quand un membre d'un groupe d'activité crée une demande de provisionnement pour une machine de cloud, vRealize Automation sélectionne une machine dans l'une des réservations disponibles pour ce groupe d'activité. Les réservations de cloud comprennent Amazon, OpenStack, vCloud Air et vCloud Director.

La réservation pour laquelle une machine est provisionnée doit répondre aux critères suivants :

- La réservation doit avoir le même type de plate-forme que le Blueprint dans lequel la machine a été demandée.
- La réservation doit être activée.
- La réservation doit disposer de capacité disponible sur son quota de machines ou disposer d'un quota illimité.

Le quota de machines alloué inclut uniquement les machines sous tension. Par exemple, si une réservation dispose d'un quota de 50 et que 40 machines ont été provisionnées, mais que seules 20 d'entre elles sont sous tension, le quota de la réservation est alloué à 40 pourcent, pas à 80 pourcent.

- La réservation doit comporter la spécification des groupes de sécurité dans la demande de machine.
- La réservation doit être associée à une région dont l'image de machine est spécifiée dans le Blueprint.
- La réservation doit disposer d'une mémoire et de ressources de stockage non allouées suffisantes pour provisionner la machine.

Dans une réservation de type Paiement à l'utilisation, les ressources peuvent être illimitées.

- Pour les machines Amazon, la demande spécifie une zone de disponibilité et si un sous-réseau doit être provisionné pour la machine dans un VPC (Virtual Private Cloud) ou un emplacement autre que VPC. La réservation doit correspondre au type de réseau (VPC ou non-VPC).

- Pour vCloud Air ou vCloud Director, si la demande spécifie un modèle d'allocation, le centre de données virtuel associé à la réservation doit avoir le même modèle d'allocation.
- Pour vCloud Director ou vCloud Air, l'organisation spécifiée doit être activée.
- Tous les modèles de Blueprints doivent être disponibles dans la réservation. Si la stratégie de réservation se mappe à plusieurs ressources, les modèles doivent être publics.
- Si le fournisseur de cloud prend en charge la sélection de réseau et que le Blueprint a des paramètres réseau spécifiques, les réseaux doivent être identiques dans la réservation.

Si le Blueprint ou la réservation spécifie un profil réseau pour l'attribution d'adresse IP statique, il est nécessaire qu'une adresse IP soit disponible pour l'attribuer à la nouvelle machine.

- Si la demande spécifie un modèle d'allocation, le modèle d'allocation de la réservation doit correspondre à celui de la demande.
- Si le Blueprint spécifie une stratégie de réservation, la réservation doit faire partie de cette stratégie de réservation.

Les stratégies de réservation permettent de garantir que la réservation sélectionnée correspond aux conditions requises pour le provisionnement de machines avec un Blueprint spécifique. Par exemple, si un Blueprint utilise une image de machine spécifique, vous pouvez utiliser des stratégies de réservation pour limiter le provisionnement aux réservations associées aux régions disposant de l'image requise.

Si aucune réservation répondant à tous les critères de sélection n'est disponible, le provisionnement échoue.

Si plusieurs réservations répondent à tous les critères, la réservation à partir de laquelle provisionner une machine demandée est déterminée par la logique suivante :

- une réservation avec une valeur de priorité inférieure est sélectionnée avant une réservation avec une valeur de priorité supérieure.
- Si plusieurs réservations ont la même priorité, la réservation avec le pourcentage de quota de machines alloué le plus bas est sélectionnée.
- Si plusieurs réservations ont une priorité et une utilisation de quota identiques, les machines sont distribuées parmi les réservations via le mécanisme Round-robin (répétition alternée).

Remarque Contrairement à la sélection Round-robin de profils réseau, la sélection Round-robin de réseaux (le cas échéant) est prise en charge et peut être associée à différents profils réseau.

Si plusieurs chemins de stockage sont disponibles sur une réservation avec une capacité suffisante pour provisionner les volumes de la machine, les chemins de stockage sont sélectionnés en fonction de la logique suivante.

- Un chemin de stockage avec une valeur de priorité inférieure est sélectionnée avant un chemin de stockage avec une valeur de priorité supérieure.
- Si le Blueprint ou la demande spécifie une stratégie de réservation de stockage, le chemin de stockage doit faire partie de cette stratégie de réservation de stockage.

Si la propriété personnalisée `VirtualMachine.DiskN.StorageReservationPolicyMode` est définie sur Non exact et qu'aucun chemin de stockage avec une capacité suffisante n'est disponible dans la stratégie de stockage, le provisionnement passe à un chemin de stockage situé à l'extérieur de la stratégie de réservation de stockage spécifiée. La valeur par défaut de `VirtualMachine.DiskN.StorageReservationPolicyMode` est Exact.

- Si plusieurs chemins de stockage ont une priorité identique, les machines sont distribuées parmi les chemins de stockage à l'aide d'une planification de type Round-robin.

Créer une réservation Amazon EC2

Vous devez attribuer des ressources aux machines en créant une réservation avant que les membres d'un groupe d'activité puissent demander le provisionnement des machines.

Vous pouvez travailler avec des réservations Amazon pour Amazon Virtual Private Cloud ou des réservations Amazon non destinées à VPC. Les utilisateurs de Amazon Web Services peuvent créer un cloud Amazon Virtual Private Cloud pour concevoir une topologie de réseau virtuel en fonction de leurs spécifications. Si vous prévoyez d'utiliser Amazon VPC, vous devez attribuer un cloud Amazon VPC à une réservation vRealize Automation. Reportez-vous à .

Lorsque vous créez une réservation Amazon ou que vous configurez un composant de machine dans le Blueprint, vous pouvez choisir parmi la liste des groupes de sécurité disponibles pour la région Amazon spécifiée. Les groupes de sécurité sont importés au moment de la collecte de données.

Remarque Après avoir créé une réservation, vous ne pouvez pas modifier les associations de groupe d'activité ou de ressource de calcul.

Pour plus d'informations sur la création d'un cloud Amazon VPC à l'aide de AWS Management Console, reportez-vous à la documentation Amazon Web Services.

Procédure

1 Spécifier les informations de réservation Amazon

Chaque réservation est configurée pour un groupe d'activité spécifique afin de lui octroyer l'accès aux machines demandées sur une ressource de calcul donnée.

2 Spécifier les paramètres de ressource et de réseau pour les réservations Amazon

Spécifiez les ressources et les paramètres réseau pour le provisionnement de machines à partir de cette réservation vRealize Automation.

3 Spécifier des propriétés personnalisées et des alertes pour les réservations Amazon

Vous pouvez associer des propriétés personnalisées à une réservation vRealize Automation. Vous pouvez également configurer des alertes pour envoyer des notifications par e-mail lorsque les ressources de réservation sont faibles.

Spécifier les informations de réservation Amazon

Chaque réservation est configurée pour un groupe d'activité spécifique afin de lui octroyer l'accès aux machines demandées sur une ressource de calcul donnée.

Remarque Après avoir créé une réservation, vous ne pouvez pas modifier les associations de groupe d'activité ou de ressource de calcul.

Vous pouvez contrôler l'affichage des réservations lors de leur ajout, de leur modification ou de leur suppression à l'aide de l'option **Filtrer par catégorie** de la page Réservations. Notez que les réservations d'agents de test n'apparaissent pas dans la liste de réservations lors d'un filtrage par catégorie.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur Fabric**.
- Vérifiez qu'un administrateur de locataire a créé au moins un groupe d'activité.
- Vérifiez qu'il existe une ressource de calcul.
- Configurez les paramètres réseau.
- (Facultatif) Configurez les informations sur le profil réseau.
- Vérifiez que vous avez accès au réseau Amazon souhaité. Par exemple, si vous souhaitez utiliser VPC, vérifiez que vous avez accès à un réseau Amazon Virtual Private Cloud (VPC).
- Vérifiez que tous les paires de clés requises existent. Reportez-vous à [Gestion des paires de clés](#).

Procédure

- 1 Sélectionnez **Infrastructure > Réservations > Réservations**.
- 2 Cliquez sur l'icône **Nouveau** (+) et sélectionnez le type de réservation que vous souhaitez créer. Sélectionnez **Amazon EC2**.
- 3 (Facultatif) Sélectionnez une réservation existante dans le menu déroulant **Copier à partir d'une réservation existante**.

Les données de la réservation sélectionnée s'affichent. Vous pouvez apporter les modifications requises pour votre nouvelle réservation.

- 4 Entrez un nom dans la zone de texte **Nom**.
- 5 Sélectionnez un locataire dans le menu déroulant **Locataire**.
- 6 Sélectionnez un groupe d'activité dans le menu déroulant **Groupe d'activité**.

Seuls les utilisateurs de ce groupe d'activité peuvent provisionner des machines à l'aide de cette réservation.

- 7 (Facultatif) Sélectionnez une stratégie de réservation dans le menu déroulant **Stratégie de réservation**.

Cette option nécessite qu'il existe une ou plusieurs stratégies de réservation. Vous pouvez modifier la réservation ultérieurement afin de spécifier une stratégie de réservation.

Celle-ci vous permet de limiter le provisionnement à des réservations spécifiques.

- 8 Entrez un chiffre dans la zone de texte **Priorité** pour définir la priorité de la réservation.

La priorité est utilisée quand un groupe d'activité dispose de plusieurs réservations. Une réservation avec la priorité 1 est utilisée pour le provisionnement avant une réservation avec la priorité 2.

- 9 (Facultatif) Décochez la case **Activer cette réservation** si vous ne souhaitez pas que cette réservation soit active.

Ne quittez pas cette page. Votre réservation n'est pas terminée.

Spécifier les paramètres de ressource et de réseau pour les réservations Amazon

Spécifiez les ressources et les paramètres réseau pour le provisionnement de machines à partir de cette réservation vRealize Automation.

Lorsque vous créez une réservation Amazon ou que vous configurez un composant de machine dans le Blueprint, vous pouvez choisir parmi la liste des groupes de sécurité disponibles pour la région du compte Amazon spécifié. Les groupes de sécurité sont importés au moment de la collecte de données. Un groupe de sécurité agit comme un pare-feu afin de contrôler l'accès à une machine. Chaque région inclut au moins le groupe de sécurité par défaut. Les administrateurs peuvent utiliser Amazon Web Services Management Console pour créer des groupes de sécurité supplémentaires, configurer des ports pour Microsoft Remote Desktop Protocol ou SSH et configurer un réseau privé virtuel pour un Amazon VPN. Pour plus d'informations sur la création et l'utilisation de groupes de sécurité dans Amazon Web Services, reportez-vous à la documentation Amazon.

Pour en savoir plus sur les équilibres de charge, reportez-vous à *Configuration de vRealize Automation*.

Prérequis

[Spécifier les informations de réservation Amazon.](#)

Procédure

- 1 Cliquez sur l'onglet **Ressources**.
- 2 Sélectionnez une ressource de calcul sur laquelle provisionner des machines dans le menu déroulant **Ressource de calcul**.

Les régions Amazon disponibles sont répertoriées.

- 3 (Facultatif) Entrez un chiffre dans la zone de texte **Quota de machines** pour définir le nombre maximal de machines pouvant être provisionnées dans cette réservation.

Seules les machines sous tension sont prises en compte dans le quota. Laissez cette zone vide pour rendre la réservation illimitée.

- 4 Sélectionnez une méthode d'attribution de paires de clés à des instances de calcul dans le menu déroulant **Paire de clés**.

Option	Description
Non spécifiée	Permet de contrôler le comportement d'une paire de clés au niveau du Blueprint plutôt qu'au niveau de la réservation.
Générée automatiquement par groupe d'activité	Chaque machine provisionnée dans un même groupe d'activité dispose d'une paire de clés identique, y compris les machines provisionnées sur d'autres réservations si elles disposent d'une ressource de calcul et d'un groupe d'activité identiques. Du fait que les paires de clés générées de cette manière sont associées à un groupe d'activité, les paires de clés sont supprimées en même temps que le groupe d'activité.
Générée automatiquement par machine	Chaque machine a une paire de clés unique. Cette méthode est la plus sécurisée, car aucune paire de clés n'est partagée entre les machines.
Paire de clés spécifique	Chaque machine provisionnée dans cette réservation dispose de la même paire de clés. Recherchez une paire de clés à utiliser avec cette réservation.

- 5 Si vous avez sélectionné **Paire de clés spécifique** dans le menu déroulant **Paire de clés**, sélectionnez une valeur de paire de clés dans le menu déroulant **Paire de clés spécifique**.
- 6 Si votre machine est configurée pour Amazon Virtual Private Cloud, cochez la case **Attribuer à un sous-réseau d'un VPC**. Sinon, laissez la case décochée.

Si vous sélectionnez l'option **Attribuer à un sous-réseau d'un VPC**, les options d'emplacement ou de sous-réseau, de groupes de sécurité et d'équilibrages de charge suivantes apparaissent dans un menu contextuel au lieu d'être affichées sur la même page.

Pour une réservation VPC, spécifiez les groupes de sécurité et les sous-réseaux de chaque VPC autorisé dans la réservation.

- 7 Sélectionnez un ou plusieurs emplacements (non-VPC) ou sous-réseaux (VPC) disponibles dans la liste **Emplacements** ou **Sous-réseaux**.

Sélectionnez chaque emplacement ou sous-réseau disponible que vous souhaitez être disponible pour le provisionnement.

- 8 Sélectionnez un ou plusieurs groupes de sécurité pouvant être attribués à une machine pendant le provisionnement dans la liste **Groupes de sécurité**.

Sélectionnez chaque groupe de sécurité pouvant être attribué à une machine lors du provisionnement. Chaque région disponible nécessite au moins un groupe de sécurité spécifié.

- 9 Sélectionnez un ou plusieurs équilibrages de charge disponibles dans la liste **Équilibrages de charge**.

Si vous utilisez la fonction d'équilibrage de charge, sélectionnez un ou plusieurs équilibrages de charge qui s'appliquent aux emplacements ou sous-réseaux sélectionnés.

Vous pouvez à présent enregistrer la réservation en cliquant sur **Enregistrer**. Sinon, vous pouvez ajouter des propriétés personnalisées à d'autres spécifications de réservation du contrôle. Vous pouvez également configurer des alertes électroniques pour envoyer des notifications lorsque les ressources allouées à cette réservation deviennent faibles.

Spécifier des propriétés personnalisées et des alertes pour les réservations Amazon

Vous pouvez associer des propriétés personnalisées à une réservation vRealize Automation. Vous pouvez également configurer des alertes pour envoyer des notifications par e-mail lorsque les ressources de réservation sont faibles.

Les propriétés personnalisées et les alertes électroniques sont des configurations facultatives de la réservation. Si vous ne souhaitez pas associer des propriétés personnalisées ou définir des alertes, cliquez sur **Enregistrer** pour terminer la création de la réservation.

Vous pouvez ajouter autant de propriétés personnalisées que vous le souhaitez.

Si vous configurez des limites, les alertes sont générées tous les jours, plutôt que lorsque les seuils spécifiés sont atteints.

Important Les notifications sont envoyées uniquement si des alertes électroniques sont configurées et que les notifications sont activées.

Prérequis

[Spécifier les paramètres de ressource et de réseau pour les réservations Amazon.](#)

Procédure

- 1 Cliquez sur l'onglet **Propriétés**.
- 2 Cliquez sur **Nouveau**.
- 3 Entrez un nom de propriété personnalisée valide.
- 4 Le cas échéant, entrez une valeur de propriété.
- 5 Cliquez sur **Enregistrer**.
- 6 (Facultatif) Ajoutez des propriétés personnalisées supplémentaires.
- 7 Cliquez sur l'onglet **Alertes**.
- 8 Cochez la case **Alertes de capacité** pour configurer les alertes à envoyer.
- 9 Utilisez le curseur pour définir des seuils pour l'allocation des ressources disponibles.
- 10 Entrez les noms d'utilisateurs ou de groupes Active Directory (et non les adresses e-mail) dans la zone de texte **Destinataires** pour recevoir des notifications d'alerte.

Entrez un nom sur chaque ligne. Appuyez sur Entrée pour séparer plusieurs entrées.

- 11 Sélectionnez **Envoyer des alertes au gestionnaire de groupes** pour inclure des gestionnaires de groupes aux alertes électroniques.

Les alertes par e-mail sont envoyées aux utilisateurs figurant dans la liste **Envoyer des e-mails du gestionnaire à** du groupe d'activité.

- 12 Spécifiez une fréquence de rappel (jours).

- 13 Cliquez sur **Enregistrer**.

La réservation est enregistrée et s'affiche dans la liste des Réservations.

Suivant

Vous pouvez configurer des stratégies de réservation facultatives ou commencer à préparer le provisionnement.

Les utilisateurs autorisés à créer des Blueprints peuvent les créer maintenant.

Créer une réservation OpenStack

Vous devez attribuer des ressources aux machines en créant une réservation avant que les membres d'un groupe d'activité puissent demander le provisionnement des machines.

Créez une réservation OpenStack.

Procédure

- 1 [Spécifier les informations de réservation OpenStack](#)

Chaque réservation est configurée pour un groupe d'activité spécifique afin de lui octroyer l'accès aux machines demandées sur une ressource de calcul donnée.

- 2 [Spécifier les paramètres de ressources et de réseau pour les réservations OpenStack](#)

Spécifiez les paramètres de ressources et de réseau disponibles pour les machines qui sont provisionnées à partir de cette réservation vRealize Automation.

- 3 [Spécifier des propriétés personnalisées et des alertes pour les réservations OpenStack](#)

Vous pouvez associer des propriétés personnalisées à une réservation vRealize Automation. Vous pouvez également configurer des alertes pour envoyer des notifications par e-mail lorsque les ressources de réservation sont faibles.

Spécifier les informations de réservation OpenStack

Chaque réservation est configurée pour un groupe d'activité spécifique afin de lui octroyer l'accès aux machines demandées sur une ressource de calcul donnée.

Remarque Après avoir créé une réservation, vous ne pouvez pas modifier les associations de groupe d'activité ou de ressource de calcul.

Vous pouvez contrôler l'affichage des réservations lors de leur ajout, de leur modification ou de leur suppression à l'aide de l'option **Filtrer par catégorie** de la page Réservations. Notez que les réservations d'agents de test n'apparaissent pas dans la liste de réservations lors d'un filtrage par catégorie.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur Fabric**.
- Vérifiez qu'un administrateur de locataire a créé au moins un groupe d'activité.
- Vérifiez qu'il existe une ressource de calcul.
- Vérifiez que tous les groupes de sécurité optionnels ou adresses IP flottantes sont configurés.
- Vérifiez que tous les paires de clés requises existent. Reportez-vous à [Gestion des paires de clés](#).
- Vérifiez qu'il existe une ressource de calcul.
- Configurez les paramètres réseau.

Procédure

- 1 Sélectionnez **Infrastructure > Réservations > Réservations**.
- 2 Cliquez sur l'icône **Nouveau** (+) et sélectionnez le type de réservation que vous souhaitez créer.
Sélectionnez **OpenStack**.
- 3 (Facultatif) Sélectionnez une réservation existante dans le menu déroulant **Copier à partir d'une réservation existante**.

Les données de la réservation sélectionnée s'affichent. Vous pouvez apporter les modifications requises pour votre nouvelle réservation.
- 4 Entrez un nom dans la zone de texte **Nom**.
- 5 Sélectionnez un locataire dans le menu déroulant **Locataire**.
- 6 Sélectionnez un groupe d'activité dans le menu déroulant **Groupe d'activité**.

Seuls les utilisateurs de ce groupe d'activité peuvent provisionner des machines à l'aide de cette réservation.
- 7 (Facultatif) Sélectionnez une stratégie de réservation dans le menu déroulant **Stratégie de réservation**.

Cette option nécessite qu'il existe une ou plusieurs stratégies de réservation. Vous pouvez modifier la réservation ultérieurement afin de spécifier une stratégie de réservation.

Celle-ci vous permet de limiter le provisionnement à des réservations spécifiques.
- 8 Entrez un chiffre dans la zone de texte **Priorité** pour définir la priorité de la réservation.

La priorité est utilisée quand un groupe d'activité dispose de plusieurs réservations. Une réservation avec la priorité 1 est utilisée pour le provisionnement avant une réservation avec la priorité 2.
- 9 (Facultatif) Décochez la case **Activer cette réservation** si vous ne souhaitez pas que cette réservation soit active.

Ne quittez pas cette page. Votre réservation n'est pas terminée.

Spécifier les paramètres de ressources et de réseau pour les réservations OpenStack

Spécifiez les paramètres de ressources et de réseau disponibles pour les machines qui sont provisionnées à partir de cette réservation vRealize Automation.

Prérequis

[Spécifier les informations de réservation OpenStack.](#)

Procédure

- 1 Cliquez sur l'onglet **Ressources**.
- 2 Sélectionnez une ressource de calcul sur laquelle provisionner des machines dans le menu déroulant **Ressource de calcul**.

Seuls les modèles situés sur le cluster que vous sélectionnez sont disponibles pour être clonés avec cette réservation.

Lors du provisionnement, les machines sont placées sur un hôte connecté au stockage local. Si la réservation utilise le stockage local, toutes les machines provisionnées par la réservation sont créées sur l'hôte qui contient ce stockage local. Cependant, si vous utilisez la propriété personnalisée `VirtualMachine.Admin.ForceHost`, qui force le provisionnement d'une machine sur un hôte différent, le provisionnement échoue. Le provisionnement échoue également si le modèle utilisé pour cloner la machine figure dans le stockage local, mais est associé à une machine appartenant à un autre cluster. Dans ce cas, l'échec est dû au fait que le provisionnement ne peut pas accéder au modèle.

- 3 (Facultatif) Entrez un chiffre dans la zone de texte **Quota de machines** pour définir le nombre maximal de machines pouvant être provisionnées dans cette réservation.

Seules les machines sous tension sont prises en compte dans le quota. Laissez cette zone vide pour rendre la réservation illimitée.

- 4 Sélectionnez une méthode d'attribution de paires de clés à des instances de calcul dans le menu déroulant **Paire de clés**.

Option	Description
Non spécifiée	Permet de contrôler le comportement d'une paire de clés au niveau du Blueprint plutôt qu'au niveau de la réservation.
Générée automatiquement par groupe d'activité	Chaque machine provisionnée dans un même groupe d'activité dispose d'une paire de clés identique, y compris les machines provisionnées sur d'autres réservations si elles disposent d'une ressource de calcul et d'un groupe d'activité identiques. Du fait que les paires de clés générées de cette manière sont associées à un groupe d'activité, les paires de clés sont supprimées en même temps que le groupe d'activité.
Générée automatiquement par machine	Chaque machine a une paire de clés unique. Cette méthode est la plus sécurisée, car aucune paire de clés n'est partagée entre les machines.
Paire de clés spécifique	Chaque machine provisionnée dans cette réservation dispose de la même paire de clés. Recherchez une paire de clés à utiliser avec cette réservation.

- 5 Si vous avez sélectionné **Paire de clés spécifique** dans le menu déroulant **Paire de clés**, sélectionnez une valeur de paire de clés dans le menu déroulant **Paire de clés spécifique**.

- 6 Sélectionnez un ou plusieurs groupes de sécurité pouvant être attribués à une machine pendant le provisionnement dans la liste **Groupes de sécurité**.
- 7 Cliquez sur l'onglet **Réseau**.
- 8 Configurez un chemin réseau pour les machines provisionnées à l'aide de cette réservation.

- a (Facultatif) Si l'option est disponible, sélectionnez un point de terminaison de stockage dans le menu déroulant **Point de terminaison**.

L'option FlexClone est visible dans la colonne des points de terminaison s'il existe un point de terminaison NetApp ONTAP et si l'hôte est virtuel. Si existe un point de terminaison NetApp ONTAP, la page de la réservation affiche le point de terminaison attribué au chemin de stockage. Lorsque vous ajoutez, mettez à jour ou supprimez un point de terminaison pour un chemin de stockage, la modification est visible dans toutes les réservations applicables.

Lorsque vous ajoutez, mettez à jour ou supprimez un point de terminaison pour un chemin de stockage, la modification est visible sur la page de la réservation.

- b Sélectionnez un chemin réseau pour les machines provisionnées par cette réservation dans la liste **Chemins d'accès au réseau**.
- c (Facultatif) Choisissez un profil réseau répertorié dans le menu déroulant **Profil réseau**.

Cette option nécessite qu'il existe un ou plusieurs profils réseau.

Vous pouvez sélectionner plusieurs chemins réseau sur une réservation, mais un seul réseau est utilisé lors du provisionnement d'une machine.

Vous pouvez à présent enregistrer la réservation en cliquant sur **Enregistrer**. Sinon, vous pouvez ajouter des propriétés personnalisées à d'autres spécifications de réservation du contrôle. Vous pouvez également configurer des alertes électroniques pour envoyer des notifications lorsque les ressources allouées à cette réservation deviennent faibles.

Spécifier des propriétés personnalisées et des alertes pour les réservations OpenStack

Vous pouvez associer des propriétés personnalisées à une réservation vRealize Automation. Vous pouvez également configurer des alertes pour envoyer des notifications par e-mail lorsque les ressources de réservation sont faibles.

Les propriétés personnalisées et les alertes électroniques sont des configurations facultatives de la réservation. Si vous ne souhaitez pas associer des propriétés personnalisées ou définir des alertes, cliquez sur **Enregistrer** pour terminer la création de la réservation.

Vous pouvez ajouter autant de propriétés personnalisées que vous le souhaitez.

Important Les notifications sont envoyées uniquement si des alertes électroniques sont configurées et que les notifications sont activées.

Si vous configurez des limites, les alertes sont générées tous les jours, plutôt que lorsque les seuils spécifiés sont atteints.

Prérequis

Spécifier les paramètres de ressources et de réseau pour les réservations OpenStack.

Procédure

- 1 Cliquez sur l'onglet **Propriétés**.
- 2 Cliquez sur **Nouveau**.
- 3 Entrez un nom de propriété personnalisée valide.
- 4 Le cas échéant, entrez une valeur de propriété.
- 5 Cliquez sur **Enregistrer**.
- 6 (Facultatif) Ajoutez des propriétés personnalisées supplémentaires.
- 7 Cliquez sur l'onglet **Alertes**.
- 8 Cochez la case **Alertes de capacité** pour configurer les alertes à envoyer.
- 9 Utilisez le curseur pour définir des seuils pour l'allocation des ressources disponibles.
- 10 Entrez les noms d'utilisateurs ou de groupes Active Directory (et non les adresses e-mail) dans la zone de texte **Destinataires** pour recevoir des notifications d'alerte.

Entrez un nom sur chaque ligne. Appuyez sur Entrée pour séparer plusieurs entrées.
- 11 Sélectionnez **Envoyer des alertes au gestionnaire de groupes** pour inclure des gestionnaires de groupes aux alertes électroniques.

Les alertes par e-mail sont envoyés aux utilisateurs figurant dans la liste **Envoyer des e-mails du gestionnaire à** du groupe d'activité.
- 12 Spécifiez une fréquence de rappel (jours).
- 13 Cliquez sur **Enregistrer**.

La réservation est enregistrée et s'affiche dans la liste des Réservations.

Suivant

Vous pouvez configurer des stratégies de réservation facultatives ou commencer à préparer le provisionnement.

Les utilisateurs autorisés à créer des Blueprints peuvent les créer maintenant.

Créer une réservation vCloud Air

Vous devez attribuer des ressources aux machines en créant une réservation vRealize Automation avant que les membres d'un groupe d'activité puissent demander le provisionnement des machines.

Chaque groupe d'activité doit avoir au moins une réservation pour ses membres afin de provisionner des machines de ce type.

Procédure

1 Spécifiez les informations de réservation de vCloud Air

Vous pouvez créer une réservation pour chaque abonnement de machine ou ressource à la demande vCloud Air. Chaque réservation est configurée pour un groupe d'activité spécifique afin de lui octroyer l'accès aux machines demandées.

2 Spécifier les ressources et les paramètres réseau pour une réservation vCloud Air

Spécifiez les ressources et les paramètres réseau accessibles aux machines vCloud Air qui sont provisionnées à partir de cette réservation vRealize Automation

3 Spécifier les propriétés et les alertes personnalisées d'une réservation vCloud Air

Vous pouvez associer des propriétés personnalisées à une réservation vRealize Automation. Vous pouvez également configurer des alertes pour envoyer des notifications par e-mail lorsque les ressources de réservation sont faibles.

Suivant

Vous pouvez configurer des stratégies de réservation facultatives ou commencer à préparer le provisionnement.

Les utilisateurs autorisés à créer des Blueprints peuvent les créer maintenant.

Spécifiez les informations de réservation de vCloud Air

Vous pouvez créer une réservation pour chaque abonnement de machine ou ressource à la demande vCloud Air. Chaque réservation est configurée pour un groupe d'activité spécifique afin de lui octroyer l'accès aux machines demandées.

Vous pouvez contrôler l'affichage des réservations lors de leur ajout, de leur modification ou de leur suppression à l'aide de l'option **Filtrer par catégorie** de la page Réservations. Notez que les réservations d'agents de test n'apparaissent pas dans la liste de réservations lors d'un filtrage par catégorie.

Remarque Après avoir créé une réservation, vous ne pouvez pas modifier les associations de groupe d'activité ou de ressource de calcul.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur Fabric**.
- Vérifiez qu'un administrateur de locataire a créé au moins un groupe d'activité.
- Vérifiez qu'il existe une ressource de calcul.
- Configurez les paramètres réseau.
- (Facultatif) Configurez les informations sur le profil réseau.

Procédure

- 1 Sélectionnez **Infrastructure > Réservations > Réservations**.

- 2 Cliquez sur l'icône **Nouveau** (+) et sélectionnez le type de réservation que vous souhaitez créer.

Les types de réservation de cloud disponibles sont Amazon, OpenStack, vCloud Air et vCloud Director.

Sélectionnez **vCloud Air**.

- 3 (Facultatif) Sélectionnez une réservation existante dans le menu déroulant **Copier à partir d'une réservation existante**.

Les données de la réservation sélectionnée s'affichent. Vous pouvez apporter les modifications requises pour votre nouvelle réservation.

- 4 Entrez un nom dans la zone de texte **Nom**.

- 5 Sélectionnez un locataire dans le menu déroulant **Locataire**.

- 6 Sélectionnez un groupe d'activité dans le menu déroulant **Groupe d'activité**.

Seuls les utilisateurs de ce groupe d'activité peuvent provisionner des machines à l'aide de cette réservation.

- 7 (Facultatif) Sélectionnez une stratégie de réservation dans le menu déroulant **Stratégie de réservation**.

Cette option nécessite qu'il existe une ou plusieurs stratégies de réservation. Vous pouvez modifier la réservation ultérieurement afin de spécifier une stratégie de réservation.

Celle-ci vous permet de limiter le provisionnement à des réservations spécifiques.

- 8 Entrez un chiffre dans la zone de texte **Priorité** pour définir la priorité de la réservation.

La priorité est utilisée quand un groupe d'activité dispose de plusieurs réservations. Une réservation avec la priorité 1 est utilisée pour le provisionnement avant une réservation avec la priorité 2.

- 9 (Facultatif) Décochez la case **Activer cette réservation** si vous ne souhaitez pas que cette réservation soit active.

Ne quittez pas cette page. Votre réservation n'est pas terminée.

Spécifier les ressources et les paramètres réseau pour une réservation vCloud Air

Spécifiez les ressources et les paramètres réseau accessibles aux machines vCloud Air qui sont provisionnées à partir de cette réservation vRealize Automation

Les modèles d'allocation de ressources disponibles pour les machines provisionnées à partir d'une réservation vCloud Director sont le pool d'allocation, le paiement à l'utilisation et le pool de réservation. Pour le paiement à l'utilisation, il n'est pas nécessaire de spécifier des volumes de stockage ou de mémoire mais vous devez définir une priorité pour le chemin d'accès au stockage. Pour plus d'informations sur ces modèles d'allocation, reportez-vous à la documentation de vCloud Air.

Vous pouvez spécifier un profil de stockage standard ou de niveau de disque. Le stockage sur disque multiniveau est disponible pour les points de terminaison vCloud Air.

Pour les intégrations utilisant SDRS (Storage Distributed Resource Scheduler), vous pouvez sélectionner un cluster de stockage afin de permettre au SDRS de gérer automatiquement l'emplacement de stockage et l'équilibrage de charge des machines provisionnées dans cette réservation. Le mode Automatisation SDRS doit être défini sur Automatique. Sinon, sélectionnez une banque de données dans le cluster pour un comportement de banque de données autonome. SDRS n'est pas pris en charge pour les périphériques de stockage FlexClone.

Remarque Les réservations définies pour les points de terminaison vCloud Air et vCloud Director ne prennent pas en charge l'utilisation de profils réseau pour le provisionnement des machines.

Prérequis

Spécifiez les informations de réservation de vCloud Director.

Procédure

- 1 Cliquez sur l'onglet **Ressources**.
- 2 Sélectionnez une ressource de calcul sur laquelle provisionner des machines dans le menu déroulant **Ressource de calcul**.

Seuls les modèles situés sur le cluster que vous sélectionnez sont disponibles pour être clonés avec cette réservation.

- 3 Sélectionnez un modèle d'allocation.
- 4 (Facultatif) Entrez un chiffre dans la zone de texte **Quota de machines** pour définir le nombre maximal de machines pouvant être provisionnées dans cette réservation.

Seules les machines sous tension sont prises en compte dans le quota. Laissez cette zone vide pour rendre la réservation illimitée.

- 5 Spécifiez la quantité de mémoire, en Go, à allouer à cette réservation dans le tableau Mémoire.

La valeur de la mémoire globale de la réservation provient de la ressource de calcul que vous avez sélectionnée.

- 6 Sélectionnez un ou plusieurs chemins de stockage répertoriés.

Les options de chemins de stockage proviennent de la ressource de calcul que vous avez sélectionnée.

- a Entrez une valeur dans la zone de texte **Cette réservation a réservé** pour spécifier la quantité de stockage à allouer à cette réservation.
- b Entrez une valeur dans la zone de texte **Priorité** pour spécifier la valeur de priorité du chemin de stockage par rapport aux autres chemins de stockage concernant cette réservation.

La priorité est utilisée en cas de chemins de stockage multiples. Un chemin de stockage avec une priorité 0 est utilisé avant un chemin avec une priorité 1.

- c Cliquez sur l'option **Désactiver** si vous ne souhaitez pas activer le chemin de stockage à utiliser par cette réservation.
- d Répétez cette étape pour configurer des clusters et des banques de données en fonction de vos besoins.

7 Cliquez sur l'onglet **Réseau**.

8 Configurez un chemin réseau pour les machines provisionnées à l'aide de cette réservation.

- a (Facultatif) Si l'option est disponible, sélectionnez un point de terminaison de stockage dans le menu déroulant **Point de terminaison**.

L'option FlexClone est visible dans la colonne des points de terminaison s'il existe un point de terminaison NetApp ONTAP et si l'hôte est virtuel. Si il existe un point de terminaison NetApp ONTAP, la page de la réservation affiche le point de terminaison attribué au chemin de stockage. Lorsque vous ajoutez, mettez à jour ou supprimez un point de terminaison pour un chemin de stockage, la modification est visible dans toutes les réservations applicables.

Lorsque vous ajoutez, mettez à jour ou supprimez un point de terminaison pour un chemin de stockage, la modification est visible sur la page de la réservation.

- b Sélectionnez un chemin réseau pour les machines provisionnées par cette réservation dans la liste **Chemins d'accès au réseau**.
- c (Facultatif) Choisissez un profil réseau répertorié dans le menu déroulant **Profil réseau**.

Cette option nécessite qu'il existe un ou plusieurs profils réseau.

Vous pouvez sélectionner plusieurs chemins réseau sur une réservation, mais un seul réseau est utilisé lors du provisionnement d'une machine.

Vous pouvez à présent enregistrer la réservation en cliquant sur **Enregistrer**. Sinon, vous pouvez ajouter des propriétés personnalisées à d'autres spécifications de réservation du contrôle. Vous pouvez également configurer des alertes électroniques pour envoyer des notifications lorsque les ressources allouées à cette réservation deviennent faibles.

Spécifier les propriétés et les alertes personnalisées d'une réservation vCloud Air

Vous pouvez associer des propriétés personnalisées à une réservation vRealize Automation. Vous pouvez également configurer des alertes pour envoyer des notifications par e-mail lorsque les ressources de réservation sont faibles.

Les propriétés personnalisées et les alertes électroniques sont des configurations facultatives de la réservation. Si vous ne souhaitez pas associer des propriétés personnalisées ou définir des alertes, cliquez sur **Enregistrer** pour terminer la création de la réservation.

Vous pouvez ajouter autant de propriétés personnalisées que vous le souhaitez.

Si vous configurez des limites, les alertes sont générées tous les jours, plutôt que lorsque les seuils spécifiés sont atteints.

Important Les notifications sont envoyées uniquement si des alertes électroniques sont configurées et que les notifications sont activées.

Les alertes ne sont pas disponibles pour les réservations de type Paiement à l'utilisation créées sans limite spécifiée.

Prérequis

[Spécifier les ressources et les paramètres réseau pour une réservation vCloud Air](#)

Procédure

- 1 Cliquez sur l'onglet **Propriétés**.
- 2 Cliquez sur **Nouveau**.
- 3 Entrez un nom de propriété personnalisée valide.
- 4 Le cas échéant, entrez une valeur de propriété.
- 5 (Facultatif) Cochez la case **Chiffré** pour chiffrer la valeur de propriété.
- 6 (Facultatif) Cochez la case **Inviter l'utilisateur** pour demander à l'utilisateur d'entrer une valeur.
Cette option ne peut pas être remplacée lors du provisionnement.
- 7 Cliquez sur **Enregistrer**.
- 8 (Facultatif) Ajoutez des propriétés personnalisées supplémentaires.
- 9 Cliquez sur l'onglet **Alertes**.
- 10 Cochez la case **Alertes de capacité** pour configurer les alertes à envoyer.
- 11 Utilisez le curseur pour définir des seuils pour l'allocation des ressources disponibles.
- 12 Entrez les noms d'utilisateurs ou de groupes Active Directory (et non les adresses e-mail) dans la zone de texte **Destinataires** pour recevoir des notifications d'alerte.
Entrez un nom sur chaque ligne. Appuyez sur Entrée pour séparer plusieurs entrées.
- 13 Sélectionnez **Envoyer des alertes au gestionnaire de groupes** pour inclure des gestionnaires de groupes aux alertes électroniques.
Les alertes par e-mail sont envoyés aux utilisateurs figurant dans la liste **Envoyer des e-mails du gestionnaire à** du groupe d'activité.
- 14 Spécifiez une fréquence de rappel (jours).
- 15 Cliquez sur **Enregistrer**.

La réservation est enregistrée et s'affiche dans la liste des Réservations.

Créer une réservation vCloud Director

Vous devez attribuer des ressources aux machines en créant une réservation vRealize Automation avant que les membres d'un groupe d'activité puissent demander le provisionnement des machines.

Chaque groupe d'activité doit avoir au moins une réservation pour ses membres afin de provisionner des machines de ce type.

Procédure

1 Spécifiez les informations de réservation de vCloud Director

Vous pouvez créer une réservation pour chaque centre de données virtuel (VDC) d'une organisation vCloud Director. Chaque réservation est configurée pour un groupe d'activité spécifique afin de lui octroyer l'accès aux machines demandées sur une ressource de calcul donnée.

2 Spécifier les ressources et les paramètres réseau pour une réservation vCloud Director

Spécifiez les ressources et les paramètres réseau accessibles aux machines vCloud Director qui sont provisionnées à partir de cette réservation vRealize Automation

3 Spécifier des propriétés personnalisées et des alertes pour les réservations vCloud Director

Vous pouvez associer des propriétés personnalisées à une réservation vRealize Automation. Vous pouvez également configurer des alertes pour envoyer des notifications par e-mail lorsque les ressources de réservation sont faibles.

Suivant

Vous pouvez configurer des stratégies de réservation facultatives ou commencer à préparer le provisionnement.

Les utilisateurs autorisés à créer des Blueprints peuvent les créer maintenant.

Spécifiez les informations de réservation de vCloud Director

Vous pouvez créer une réservation pour chaque centre de données virtuel (VDC) d'une organisation vCloud Director. Chaque réservation est configurée pour un groupe d'activité spécifique afin de lui octroyer l'accès aux machines demandées sur une ressource de calcul donnée.

Vous pouvez contrôler l'affichage des réservations lors de leur ajout, de leur modification ou de leur suppression à l'aide de l'option **Filtrer par catégorie** de la page Réservations. Notez que les réservations d'agents de test n'apparaissent pas dans la liste de réservations lors d'un filtrage par catégorie.

Remarque Après avoir créé une réservation, vous ne pouvez pas modifier les associations de groupe d'activité ou de ressource de calcul.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur Fabric**.
- Vérifiez qu'un administrateur de locataire a créé au moins un groupe d'activité.
- Vérifiez qu'il existe une ressource de calcul.
- Configurez les paramètres réseau.

- (Facultatif) Configurez les informations sur le profil réseau.

Procédure

- 1 Sélectionnez **Infrastructure > Réservations > Réservations**.
- 2 Cliquez sur l'icône **Nouveau** (+) et sélectionnez le type de réservation que vous souhaitez créer.
Les types de réservation de cloud disponibles sont Amazon, OpenStack, vCloud Air et vCloud Director.
Sélectionnez **vCloud Director**.
- 3 (Facultatif) Sélectionnez une réservation existante dans le menu déroulant **Copier à partir d'une réservation existante**.
Les données de la réservation sélectionnée s'affichent. Vous pouvez apporter les modifications requises pour votre nouvelle réservation.
- 4 Entrez un nom dans la zone de texte **Nom**.
- 5 Sélectionnez un locataire dans le menu déroulant **Locataire**.
- 6 Sélectionnez un groupe d'activité dans le menu déroulant **Groupe d'activité**.
Seuls les utilisateurs de ce groupe d'activité peuvent provisionner des machines à l'aide de cette réservation.
- 7 (Facultatif) Sélectionnez une stratégie de réservation dans le menu déroulant **Stratégie de réservation**.
Cette option nécessite qu'il existe une ou plusieurs stratégies de réservation. Vous pouvez modifier la réservation ultérieurement afin de spécifier une stratégie de réservation.
Celle-ci vous permet de limiter le provisionnement à des réservations spécifiques.
- 8 Entrez un chiffre dans la zone de texte **Priorité** pour définir la priorité de la réservation.
La priorité est utilisée quand un groupe d'activité dispose de plusieurs réservations. Une réservation avec la priorité 1 est utilisée pour le provisionnement avant une réservation avec la priorité 2.
- 9 (Facultatif) Décochez la case **Activer cette réservation** si vous ne souhaitez pas que cette réservation soit active.

Ne quittez pas cette page. Votre réservation n'est pas terminée.

Spécifier les ressources et les paramètres réseau pour une réservation vCloud Director

Spécifiez les ressources et les paramètres réseau accessibles aux machines vCloud Director qui sont provisionnées à partir de cette réservation vRealize Automation

Les modèles d'allocation de ressources disponibles pour les machines provisionnées à partir d'une réservation vCloud Director sont le pool d'allocation, le paiement à l'utilisation et le pool de réservation. Pour le paiement à l'utilisation, il n'est pas nécessaire de spécifier des volumes de stockage ou de mémoire mais vous devez définir une priorité pour le chemin d'accès au stockage. Pour plus d'informations sur ces modèles d'allocation, reportez-vous à la documentation de vCloud Director.

Vous pouvez spécifier un profil de stockage standard ou de niveau de disque. Un stockage sur disque multiniveau est disponible pour les points de terminaison de vCloud Director 5.6 et des versions supérieures. Le stockage sur disque multiniveau n'est pas pris en charge pour les points de terminaison de vCloud Director 5.5.

Pour les intégrations utilisant SDRS (Storage Distributed Resource Scheduler), vous pouvez sélectionner un cluster de stockage afin de permettre au SDRS de gérer automatiquement l'emplacement de stockage et l'équilibrage de charge des machines provisionnées dans cette réservation. Le mode Automatisation SDRS doit être défini sur Automatique. Sinon, sélectionnez une banque de données dans le cluster pour un comportement de banque de données autonome. SDRS n'est pas pris en charge pour les périphériques de stockage FlexClone.

Remarque Les réservations définies pour les points de terminaison vCloud Air et vCloud Director ne prennent pas en charge l'utilisation de profils réseau pour le provisionnement des machines.

Prérequis

Spécifiez les informations de réservation de vCloud Director.

Procédure

1 Cliquez sur l'onglet **Ressources**.

2 Sélectionnez une ressource de calcul sur laquelle provisionner des machines dans le menu déroulant **Ressource de calcul**.

Seuls les modèles situés sur le cluster que vous sélectionnez sont disponibles pour être clonés avec cette réservation.

3 Sélectionnez un modèle d'allocation.

4 (Facultatif) Entrez un chiffre dans la zone de texte **Quota de machines** pour définir le nombre maximal de machines pouvant être provisionnées dans cette réservation.

Seules les machines sous tension sont prises en compte dans le quota. Laissez cette zone vide pour rendre la réservation illimitée.

5 Spécifiez la quantité de mémoire, en Go, à allouer à cette réservation dans le tableau Mémoire.

La valeur de la mémoire globale de la réservation provient de la ressource de calcul que vous avez sélectionnée.

6 Sélectionnez un ou plusieurs chemins de stockage répertoriés.

Les options de chemins de stockage proviennent de la ressource de calcul que vous avez sélectionnée.

- a Entrez une valeur dans la zone de texte **Cette réservation a réservé** pour spécifier la quantité de stockage à allouer à cette réservation.
- b Entrez une valeur dans la zone de texte **Priorité** pour spécifier la valeur de priorité du chemin de stockage par rapport aux autres chemins de stockage concernant cette réservation.

La priorité est utilisée en cas de chemins de stockage multiples. Un chemin de stockage avec une priorité 0 est utilisé avant un chemin avec une priorité 1.

- c Cliquez sur l'option **Désactiver** si vous ne souhaitez pas activer le chemin de stockage à utiliser par cette réservation.
- d Répétez cette étape pour configurer des clusters et des banques de données en fonction de vos besoins.

7 Cliquez sur l'onglet **Réseau**.

8 Configurez un chemin réseau pour les machines provisionnées à l'aide de cette réservation.

- a (Facultatif) Si l'option est disponible, sélectionnez un point de terminaison de stockage dans le menu déroulant **Point de terminaison**.

L'option FlexClone est visible dans la colonne des points de terminaison s'il existe un point de terminaison NetApp ONTAP et si l'hôte est virtuel. Si existe un point de terminaison NetApp ONTAP, la page de la réservation affiche le point de terminaison attribué au chemin de stockage. Lorsque vous ajoutez, mettez à jour ou supprimez un point de terminaison pour un chemin de stockage, la modification est visible dans toutes les réservations applicables.

Lorsque vous ajoutez, mettez à jour ou supprimez un point de terminaison pour un chemin de stockage, la modification est visible sur la page de la réservation.

- b Sélectionnez un chemin réseau pour les machines provisionnées par cette réservation dans la liste **Chemins d'accès au réseau**.
- c (Facultatif) Choisissez un profil réseau répertorié dans le menu déroulant **Profil réseau**.

Cette option nécessite qu'il existe un ou plusieurs profils réseau.

Vous pouvez sélectionner plusieurs chemins réseau sur une réservation, mais un seul réseau est utilisé lors du provisionnement d'une machine.

Vous pouvez à présent enregistrer la réservation en cliquant sur **Enregistrer**. Sinon, vous pouvez ajouter des propriétés personnalisées à d'autres spécifications de réservation du contrôle. Vous pouvez également configurer des alertes électroniques pour envoyer des notifications lorsque les ressources allouées à cette réservation deviennent faibles.

Spécifier des propriétés personnalisées et des alertes pour les réservations vCloud Director

Vous pouvez associer des propriétés personnalisées à une réservation vRealize Automation. Vous pouvez également configurer des alertes pour envoyer des notifications par e-mail lorsque les ressources de réservation sont faibles.

Les propriétés personnalisées et les alertes électroniques sont des configurations facultatives de la réservation. Si vous ne souhaitez pas associer des propriétés personnalisées ou définir des alertes, cliquez sur **Enregistrer** pour terminer la création de la réservation.

Vous pouvez ajouter autant de propriétés personnalisées que vous le souhaitez.

Si vous configurez des limites, les alertes sont générées tous les jours, plutôt que lorsque les seuils spécifiés sont atteints.

Important Les notifications sont envoyées uniquement si des alertes électroniques sont configurées et que les notifications sont activées.

Les alertes ne sont pas disponibles pour les réservations de type Paiement à l'utilisation créées sans limite spécifiée.

Prérequis

[Spécifier les ressources et les paramètres réseau pour une réservation vCloud Director.](#)

Procédure

- 1 Cliquez sur l'onglet **Propriétés**.
- 2 Cliquez sur **Nouveau**.
- 3 Entrez un nom de propriété personnalisée valide.
- 4 Le cas échéant, entrez une valeur de propriété.
- 5 (Facultatif) Cochez la case **Chiffré** pour chiffrer la valeur de propriété.
- 6 (Facultatif) Cochez la case **Inviter l'utilisateur** pour demander à l'utilisateur d'entrer une valeur.
Cette option ne peut pas être remplacée lors du provisionnement.
- 7 Cliquez sur **Enregistrer**.
- 8 (Facultatif) Ajoutez des propriétés personnalisées supplémentaires.
- 9 Cliquez sur l'onglet **Alertes**.
- 10 Cochez la case **Alertes de capacité** pour configurer les alertes à envoyer.
- 11 Utilisez le curseur pour définir des seuils pour l'allocation des ressources disponibles.
- 12 Entrez les noms d'utilisateurs ou de groupes Active Directory (et non les adresses e-mail) dans la zone de texte **Destinataires** pour recevoir des notifications d'alerte.
Entrez un nom sur chaque ligne. Appuyez sur Entrée pour séparer plusieurs entrées.

- 13** Sélectionnez **Envoyer des alertes au gestionnaire de groupes** pour inclure des gestionnaires de groupes aux alertes électroniques.

Les alertes par e-mail sont envoyées aux utilisateurs figurant dans la liste **Envoyer des e-mails du gestionnaire à** du groupe d'activité.

- 14** Spécifiez une fréquence de rappel (jours).

- 15** Cliquez sur **Enregistrer**.

La réservation est enregistrée et s'affiche dans la liste des Réservations.

Créer une réservation pour Microsoft Azure

Créez une réservation Azure pour un groupe d'activité spécifique afin d'octroyer aux utilisateurs de ce groupe la possibilité de demander des machines virtuelles Azure sur une ressource de calcul donnée.

Si votre déploiement prend en charge Single Sign-On par le biais d'un tunnel VPN, vous pouvez configurer la prise en charge de cette fonctionnalité par des machines virtuelles Azure en utilisant les paramètres de l'onglet Propriétés.

Remarque Ignorez l'onglet Alertes lors de la création d'une réservation Azure, car il ne s'applique pas. Après avoir créé une réservation, vous ne pouvez pas modifier les associations de groupe d'activité. Également, contrairement aux autres types de machine, il n'y a pas de lien direct entre une réservation Azure et un Blueprint.

Vous pouvez contrôler l'affichage des réservations lors de leur ajout, de leur modification ou de leur suppression à l'aide de l'option **Filtrer par catégorie** de la page Réservations. Notez que les réservations d'agents de test n'apparaissent pas dans la liste de réservations lors d'un filtrage par catégorie.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur Fabric**.
- Vérifiez qu'un administrateur de locataire a créé au moins un groupe d'activité.
- (Facultatif) Configurez les informations sur le profil réseau.
- Vérifiez que vous avez accès aux ressources Azure requises.
- Vérifiez que toutes les paires de clés requises existent. Pour obtenir des informations sur les paires de clés, reportez-vous à la section *Configuration de vRealize Automation*.
- Obtenez un ID d'abonnement Azure valide qui corresponde à celui qui est utilisé avec le point de terminaison Azure concerné. Si vous utilisez plusieurs abonnements Azure, vous devez créer une réservation pour chacun de ces derniers.
- Si votre déploiement prend en charge Single Sign-On par le biais d'un tunnel VPN, vous devez configurer la connectivité VPC appropriée avant de créer une réservation. Reportez-vous à [Configurer la connectivité VPC entre le réseau et Azure](#).

Configurer les informations de réservation de base Microsoft Azure

Spécifiez les informations de base d'une réservation Microsoft Azure.

Toutes les informations indiquées sur la page **Réservation** sont requises, à l'exception de la stratégie de réservation. Toutes les informations sur les pages relatives à la réservation Azure suivantes sont facultatives.

Procédure

- 1 Sélectionnez **Infrastructure > Administration > Réservations**.
- 2 Cliquez sur l'icône **Nouveau** (+) et sélectionnez le type de réservation que vous souhaitez créer.
Sélectionnez **Azure**.
- 3 (Facultatif) Sélectionnez une réservation existante dans le menu déroulant **Copier à partir d'une réservation existante**.

Les données de la réservation sélectionnée s'affichent. Vous pouvez apporter les modifications requises pour votre nouvelle réservation.
- 4 Entrez un nom dans la zone de texte **Nom**.
- 5 Sélectionnez un groupe d'activité dans le menu déroulant **Groupe d'activité**.

Seuls les utilisateurs de ce groupe d'activité peuvent provisionner des machines à l'aide de cette réservation.
- 6 Ignorez la zone de texte **Stratégie de réservation**, car elle ne s'applique pas aux réservations Azure.
- 7 Entrez un chiffre dans la zone de texte **Priorité** pour définir la priorité de la réservation.

La priorité est utilisée quand un groupe d'activité dispose de plusieurs réservations. Une réservation avec la priorité 1 est utilisée pour le provisionnement avant une réservation avec la priorité 2.
- 8 (Facultatif) Décochez la case **Activer cette réservation** si vous ne souhaitez pas que cette réservation soit active.
- 9 Cliquez sur **OK**.

Configurer les informations des ressources de réservation Azure

Lors de la définition d'une réservation Azure, vous pouvez affecter des informations sur le groupe de ressources et le compte de stockage en fonction de l'instance Azure que vous utilisez. Lorsque vous créez une réservation, la logique de provisionnement de vRealize Automation tente d'affecter des ressources, telles que des groupes de ressources et des comptes de stockage, en fonction des informations de ressource spécifiées par la réservation pendant le provisionnement d'une machine virtuelle.

Vous pouvez configurer les informations relatives au groupe de ressources et au compte de stockage d'une machine virtuelle Azure appartenant à la réservation. Toutefois, il est également possible de laisser ces champs vides dans la réservation. Si vous laissez les champs vides, les informations du groupe de ressources par défaut et du compte de stockage sont relatives à l'identifiant d'abonnement Azure spécifié et sont utilisées pour tous les Blueprints correspondants. Vous pouvez également mettre à jour ces informations lors de la création d'un Blueprint ou lors du provisionnement d'une machine virtuelle.

Prérequis

Obtenez l'identifiant d'abonnement pour votre instance Azure.

Procédure

1 Tapez ou collez votre identifiant d'abonnement Azure dans la zone de texte **ID d'abonnement**.

2 Sélectionnez l'emplacement de la réservation en cliquant sur la liste déroulante **Emplacement**.

Vous pouvez laisser ce champ vide pour créer une réservation sans lien avec l'emplacement. Dans le cas contraire, vous devez spécifier l'emplacement lors de la création d'un Blueprint ou lors du provisionnement d'Azure sur une machine virtuelle.

3 Cliquez sur **Nouveau** dans la table des groupes de ressources.

a Collez les informations relatives au groupe de ressources de votre instance Azure dans la zone de texte **Nom**.

Remarque La zone **Nom** ne doit pas rester vide.

b Affectez une valeur numérique de propriété dans la zone de texte **Priorité**.

Cette affectation détermine la priorité lorsqu'un groupe de ressources comporte lui-même plusieurs autres groupes de ressources, les nombres inférieurs étant prioritaires.

c Cliquez sur **Enregistrer** pour ajouter le groupe de ressources à la réservation.

4 Cliquez sur **Nouveau** dans la table des comptes de stockage.

a Collez les informations relatives au nom de compte de stockage de votre instance Azure dans la zone de texte **Nom**.

Remarque La zone **Nom** ne doit pas rester vide.

b Affectez une valeur numérique de propriété dans la zone de texte **Priorité**.

c Cliquez sur **Enregistrer** pour ajouter le compte de stockage à la réservation.

Cette affectation détermine la priorité lorsqu'une réservation comporte plusieurs comptes de stockage, les nombres inférieurs étant prioritaires.

5 Cliquez sur **OK** pour passer à l'onglet suivant.

Configurer les propriétés Azure

Vous pouvez ajouter des propriétés personnalisées à une réservation Azure pour prendre en charge des options, telles que le tunnel VPN permettant de gérer la communication entre plusieurs réseaux. Cette fonctionnalité facilite également l'ajout de composants logiciels aux Blueprints.

Vous devez créer des propriétés personnalisées qui définissent les URL appropriées pour prendre en charge le tunnel VPN sur votre réseau. En outre, vous devez créer les propriétés qui définissent le chemin d'accès aux scripts de configuration du tunnel Azure précédemment téléchargés.

Utilisez l'adresse IP privée de la machine physique de votre tunnel Azure et le port 1443, que vous avez attribué pour *vRealize_automation_appliance_fqdn* en appelant le tunnel SSH.

Le tableau suivant affiche les noms et les valeurs des propriétés requises pour prendre en charge le tunnel VPN.

Nom	Valeur
Azure.Windows.ScriptPath	Spécifie le chemin d'accès au script téléchargé qui configure la tunnellation pour les systèmes Windows. Mettez le chemin d'accès à jour en fonction de votre déploiement.
Azure.Linux.ScriptPath	Spécifie le chemin d'accès au script téléchargé qui configure la tunnellation pour les systèmes Linux. Mettez le chemin d'accès à jour en fonction de votre déploiement.
agent.download.url	Spécifie l'URL de l'agent VPN sur votre déploiement. Le format de l'URL est <code>https:// Private_IP:1443/software-service//resources/noble-agent.jar</code>
software.agent.service.url	Entrez l'URL du service de l'agent logiciel VPN pour votre déploiement ; le format de l'URL est <code>https:// Private_IP:1443/software-service/api</code>
software.ebs.url	Entrez l'URL du service Broker pour l'événement pour votre déploiement. Le format de l'URL est <code>https:// Private_IP:1443/event-broker-service/api</code>

Prérequis

- Téléchargez les scripts Azure fournis par VMware sur la page **Programmes d'installation d'agents invités et logiciels** de votre dispositif vRealize Automation.

Ces scripts installent les extensions Azure requises pour prendre en charge le tunnel VPN. Il existe deux scripts : `script.ps1` et `script.sh`. Le fichier `.ps1` est destiné aux systèmes Windows, et le fichier `.sh` est destiné aux systèmes Linux.

- Exécutez `https://vrealize-automation-appliance-fqdn/software` pour ouvrir la page du dispositif vRealize Automation VMware.
- Cliquez sur le lien **Agents invités et logiciels** sous l'en-tête Pour installer des composants de vRealize Automation (IaaS, agents invités et logiciels, outils).
- Téléchargez les fichiers de script Azure sous l'en-tête Machines Azure. Enregistrez les fichiers de script dans un emplacement approprié. Vous devez pointer vers cet emplacement lors de la configuration des propriétés personnalisées de réservation Azure.

Procédure

- 1 Cliquez sur l'onglet **Propriétés**.
- 2 Cliquez sur **Nouveau**.
- 3 Entrez le nom et la valeur appropriés de la propriété personnalisée dans la boîte de dialogue Propriétés.
- 4 Lorsque vous créez une propriété, cliquez sur **OK** dans la boîte de dialogue pour l'ajouter.

- 5 Lorsque vous avez terminé d'ajouter toutes les propriétés requises, cliquez sur **OK** pour enregistrer vos paramètres.

Suivant

Une fois que vous avez créé des propriétés personnalisées pour prendre en charge le tunnel VPN, vous pouvez créer des composants logiciels pour vos Blueprints Azure. Consultez *Configuration de vRealize Automation* pour plus d'informations.

Lorsque vous configurez un composant logiciel pour Azure, sélectionnez **Machine virtuelle Azure** dans le menu déroulant Conteneur sur la page Nouveau logiciel.

Configurer les informations réseau de réservation Azure

Vous pouvez configurer les informations de réseau virtuel et d'équilibrage de charge pour une machine virtuelle Azure depuis la réservation.

Vous pouvez également choisir de laisser cette page partiellement ou totalement vide, et de configurer les informations de réseau virtuel et d'équilibrage de charge lorsque vous provisionnez une machine virtuelle.

Si vous spécifiez un profil réseau sans préciser de sous-réseau, le nom de la première plage réseau existante du profil réseau spécifié est utilisé en tant que nom de sous-réseau. Si un profil réseau est spécifié, vous pouvez laisser la zone de texte vNet vide. Dans ce cas, le nom de la première plage réseau du profil réseau spécifié est utilisé en tant que nom de sous-réseau, tandis que le nom de réseau virtuel est résolu en fonction du premier réseau virtuel Azure contenant un sous-réseau adapté.

Prérequis

Vous devez obtenir les informations appropriées de réseau virtuel et d'équilibrage de charge depuis votre instance Azure le cas échéant.

Procédure

- 1 Cliquez sur **Nouveau** dans la table Réseaux pour configurer le réseau virtuel Azure approprié à utiliser avec votre machine virtuelle.
 - a Collez les informations appropriées de nom de réseau virtuel depuis votre instance Azure dans la zone de texte **vNet**.
 - b Collez les informations appropriées de nom de sous-réseau depuis votre instance Azure dans la zone de texte **Sous-réseau**.
 La spécification Sous-réseau est facultative. Si cette case reste vide, le sous-réseau du réseau virtuel spécifié est utilisé par défaut.
 - c Tapez ou collez le nom approprié dans la zone de texte **Profil réseau**. Vous pouvez utiliser le profil réseau dans le Blueprint pour associer une carte d'interface réseau à un réseau.
 La spécification du profil réseau est facultative. Utilisez-la pour créer un Blueprint sur le profil réseau défini dans vRealize Automation au lieu de l'associer aux constructions réseau d'Azure.

- d Affectez une valeur numérique de propriété dans la zone de texte **Priorité** le cas échéant.
Cette affectation détermine la priorité lorsqu'un réseau virtuel comporte plusieurs réservations, les nombres inférieurs étant prioritaires.
- e Cliquez sur **Enregistrer** pour ajouter le groupe de ressources à la réservation.
- 2 Cliquez sur **Nouveau** dans la table d'équilibrage de charge si vous déployez plusieurs machines et procédez à l'équilibrage de charge.
 - a Collez le nom du système d'équilibrage de charge provenant de votre instance Azure dans la zone de texte **Nom**.
 - b Collez le nom approprié de votre instance Azure dans la zone de texte **Pool d'adresses du serveur principal**.
 - c Affectez une valeur numérique de propriété dans la zone de texte **Priorité** le cas échéant.
Cette affectation détermine la priorité lorsqu'un réseau virtuel comporte plusieurs systèmes d'équilibrage de charge, les nombres inférieurs étant prioritaires.
 - d Cliquez sur **Enregistrer** pour ajouter le système d'équilibrage de charge à la réservation.
- 3 Cliquez sur **Nouveau** dans la table de groupes de sécurité si vous déployez plusieurs machines qui doivent communiquer à travers un pare-feu.
 - a Collez le nom du groupe de sécurité provenant de votre instance Azure dans la zone de texte **Nom**.
 - b Affectez une valeur numérique de propriété dans la zone de texte **Priorité** le cas échéant.
Cette affectation détermine la priorité lorsqu'un réseau virtuel comporte plusieurs groupes de sécurité, les nombres inférieurs étant prioritaires.
 - c Cliquez sur **Enregistrer** pour ajouter le groupe de sécurité à la réservation.
- 4 Cliquez sur **OK**.

Scénario : créer une réservation Amazon pour un environnement de validation technique

Étant donné que vous avez utilisé un tunnel SSH pour établir une connexion temporaire entre le réseau et Amazon VPC pour l'environnement de validation technique, ajoutez des propriétés personnalisées aux réservations Amazon afin de garantir que l'agent de démarrage Logiciel et l'agent invité exécutent des communications via le tunnel.

La connectivité entre le réseau et Amazon VPC n'est obligatoire que si vous souhaitez utiliser l'agent invité pour personnaliser les machines provisionnées, ou si vous souhaitez inclure à des Blueprints des composants Logiciel. Dans un environnement de production, vous configureriez cette connectivité de façon officielle par le biais de Amazon Web Services. Cependant, puisque vous travaillez dans un environnement de validation technique, vous avez configuré un tunnel SSH temporaire.

À l'aide de vos privilèges d'administrateur Fabric, créez une réservation afin d'allouer les ressources Amazon Web Services et incluez plusieurs propriétés personnalisées pour prendre en charge la réalisation du tunnel SSH. Configurez également la réservation sur la même région et le même VPC que la machine tunnel.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur Fabric**.
- Configurez un tunnel SSH afin d'établir une connectivité entre le réseau et Amazon VPC. Notez le sous-réseau, le groupe de sécurité et l'adresse IP privée de la machine tunnel Amazon AWS. Reportez-vous à [Scénario : configurer la connectivité VPC entre le réseau et Amazon pour un environnement de validation technique](#).
- Créez un groupe d'activité pour les membres de votre service informatique qui doivent concevoir des Blueprints dans l'environnement de validation technique. Reportez-vous à [Créer un groupe d'activité](#).
- Vérifiez qu'un administrateur de locataire a créé au moins un groupe d'activité.

Procédure

1 [Scénario : spécifier des informations de réservation Amazon AWS pour un environnement de validation technique](#)

Vous souhaitez réserver des ressources pour l'équipe d'architectes de Blueprint afin qu'elle puisse tester ses fonctionnalités dans l'environnement de validation technique. Pour ce faire, configurez la réservation afin d'allouer des ressources au groupe d'activité des architectes.

2 [scénario : spécifier les paramètres réseau Amazon AWS dans un environnement de validation technique](#)

Configurez la réservation de sorte qu'elle utilise les mêmes paramètres de région et de mise en réseau que ceux de la machine tunnel. De plus, restreignez le nombre de machines qui peuvent être mises sous tension dans cette réservation, afin de gérer l'utilisation des ressources.

3 [Scénario : spécifier des propriétés personnalisées pour que les agents exécutent des communications via le tunnel](#)

Lors de la configuration de la connectivité entre le réseau et Amazon VPC, vous avez configuré un transfert de port qui permet à votre machine tunnel Amazon AWS d'accéder aux ressources vRealize Automation.

Scénario : spécifier des informations de réservation Amazon AWS pour un environnement de validation technique

Vous souhaitez réserver des ressources pour l'équipe d'architectes de Blueprint afin qu'elle puisse tester ses fonctionnalités dans l'environnement de validation technique. Pour ce faire, configurez la réservation afin d'allouer des ressources au groupe d'activité des architectes.

Remarque Après avoir créé une réservation, vous ne pouvez pas modifier les associations de groupe d'activité ou de ressource de calcul.

Procédure

- 1 Sélectionnez **Infrastructure > Réservations > Réservations**.
- 2 Cliquez sur l'icône **Nouveau** (+) et sélectionnez le type de réservation que vous souhaitez créer. Sélectionnez **Amazon**.

- 3 Dans la zone de texte **Nom**, entrez **Validation technique du tunnel Amazon**.
- 4 Dans le menu déroulant **Groupe d'activité**, sélectionnez le groupe que vous avez créé pour les architectes du Blueprint.
- 5 Dans la zone de texte **Priorité**, entrez le chiffre **1** pour accorder à cette réservation le niveau de priorité le plus élevé.

Vous avez configuré le groupe d'activité et la priorité de la réservation. Il vous reste à allouer des ressources et à configurer les propriétés personnalisées du tunnel SSH.

scénario : spécifier les paramètres réseau Amazon AWS dans un environnement de validation technique

Configurez la réservation de sorte qu'elle utilise les mêmes paramètres de région et de mise en réseau que ceux de la machine tunnel. De plus, restreignez le nombre de machines qui peuvent être mises sous tension dans cette réservation, afin de gérer l'utilisation des ressources.

Procédure

- 1 Cliquez sur l'onglet **Ressources**.
- 2 Sélectionnez une ressource de calcul sur laquelle provisionner des machines dans le menu déroulant **Ressource de calcul**.

Sélectionnez la région Amazon AWS dans laquelle réside la machine tunnel.
- 3 (Facultatif) Entrez un chiffre dans la zone de texte **Quota de machines** pour définir le nombre maximal de machines pouvant être provisionnées dans cette réservation.

Seules les machines sous tension sont prises en compte dans le quota. Laissez cette zone vide pour rendre la réservation illimitée.
- 4 Dans le menu déroulant **Paire de clés**, sélectionnez **Spécifier une paire de clés**.

Puisqu'il s'agit d'un environnement de validation technique, choisissez une seule paire de clés pour toutes les machines provisionnées à l'aide de cette réservation.
- 5 Dans le menu déroulant **Paire de clés**, sélectionnez la paire de clés à partager avec les utilisateurs architectes.
- 6 Cochez la case **Attribuer à un sous-réseau d'un VPC**.
- 7 Sélectionnez un sous-réseau et des groupes de sécurité identiques à ceux que la machine tunnel utilise.

Vous avez configuré la réservation pour qu'elle utilise les mêmes paramètres de région et de mise en réseau que ceux de la machine tunnel. Cependant, vous devez ajouter des propriétés personnalisées pour que l'agent de démarrage et l'agent invité Logiciel exécutent des communications par le biais du tunnel.

Scénario : spécifier des propriétés personnalisées pour que les agents exécutent des communications via le tunnel

Lors de la configuration de la connectivité entre le réseau et Amazon VPC, vous avez configuré un transfert de port qui permet à votre machine tunnel Amazon AWS d'accéder aux ressources vRealize Automation.

Vous devez ajouter des propriétés personnalisées de tunnel à la réservation pour configurer les agents afin qu'ils accèdent à ces ports.

Remarque Si vous utilisez un réseau système PAT ou NAT entre le réseau de votre organisation et le réseau vRealize Automation, vous pouvez utiliser ces propriétés pour l'accès à votre port et à votre adresse IP privée.

Procédure

- 1 Cliquez sur l'onglet **Propriétés**.
- 2 Cliquez sur **Nouveau**.
- 3 Configurez les propriétés personnalisées du tunnel.

Utilisez l'adresse IP privée de la machine tunnel Amazon AWS et le port 1443, que vous avez attribué à `vRealize_automation_appliance_fqdn` en appelant le tunnel SSH.

Option	Valeur
<code>software.ebs.url</code>	<code>https://Private_IP:1443/event-broker-service/api</code>
<code>software.agent.service.url</code>	<code>https://Private_IP:1443/software-service/api</code>
<code>agent.download.url</code>	<code>https://Private_IP:1443/software-service/resources/nobel-agent.jar</code>

- 4 Cliquez sur **Enregistrer**.

Vous avez créé une réservation afin d'allouer des ressources Amazon AWS au groupe d'activité des architectes. Vous avez configuré la réservation pour prendre en charge l'agent invité et l'agent de démarrage Logiciel. Les architectes peuvent créer des Blueprints capables d'utiliser l'agent invité pour personnaliser des machines déployées ou pour inclure des composants Logiciel.

Création de catégories de réservations virtuelles

Une réservation de type de catégorie virtuelle fournit un accès aux services de provisionnement d'un déploiement de machine virtuelle pour un groupe d'activité vRealize Automation particulier. Les types de réservation virtuelle disponibles incluent vSphere, Hyper-V, KVM, SCVMM et XenServer.

Une réservation est un partage de la mémoire, du CPU, de la mise en réseau et des ressources de stockage d'une ressource de calcul allouée à un groupe d'activité vRealize Automation particulier.

Un groupe d'activité peut avoir plusieurs réservations sur un point de terminaison ou des réservations sur plusieurs points de terminaison.

Pour provisionner des machines virtuelles, un groupe d'activités doit disposer d'au moins une réservation sur une ressource de calcul virtuelle. Chaque réservation concerne un seul groupe d'activité, mais un groupe d'activité peut avoir plusieurs réservations sur une seule ressource de calcul ou plusieurs réservations sur des ressources de calcul de différents types.

En plus de définir le partage des ressources Fabric attribuées au groupe d'activité, une réservation peut définir des stratégies, des priorités et des quotas qui déterminent le placement de la machine.

Pour réussir le provisionnement, la réservation doit disposer de suffisamment de stockage. La disponibilité de stockage de la réservation dépend des conditions suivantes :

- Quantité de stockage disponible sur la banque de données/cluster.
- Quantité de stockage réservée pour cette banque de données/cluster.
- Quantité de stockage déjà allouée dans vRealize Automation

Par exemple, même si l'instance de vCenter Server dispose de stockage pour la banque de données/cluster, si un stockage suffisant n'est pas réservé dans la réservation, le provisionnement échoue avec l'erreur « Aucune réservation n'est disponible pour l'allocation... ». Le stockage alloué sur une réservation dépend du nombre de machines virtuelles (quel que soit leur état) sur cette réservation spécifique. Consultez l'article de la base de connaissances VMware *Machine XXX : Aucune réservation n'est disponible à allouer au sein du groupe XXX. Un stockage total de XX Go a été demandé (2151030)* à l'adresse <http://kb.vmware.com/kb/2151030> pour plus d'informations.

Présentation de la logique de sélection pour les réservations

Quand un membre d'un groupe d'activité crée une demande de provisionnement pour une machine virtuelle, vRealize Automation sélectionne une machine dans l'une des réservations disponibles pour ce groupe d'activité.

La réservation pour laquelle une machine est provisionnée doit répondre aux critères suivants :

- La réservation doit avoir le même type de plate-forme que le Blueprint dans lequel la machine a été demandée.

Un Blueprint virtuel générique peut être provisionné sur n'importe quel type de réservation virtuelle.

- La réservation doit être activée.
- La ressource de calcul doit être accessible et non en mode de maintenance.
- La réservation doit disposer de capacité disponible sur son quota de machines ou disposer d'un quota illimité.

Le quota de machines alloué inclut uniquement les machines sous tension. Par exemple, si une réservation dispose d'un quota de 50 et que 40 machines ont été provisionnées, mais que seules 20 d'entre elles sont sous tension, le quota de la réservation est alloué à 40 pourcent, pas à 80 pourcent.

- La réservation doit disposer d'une mémoire et de ressources de stockage non allouées suffisantes pour provisionner la machine.

Quand le quota, la mémoire ou le stockage de machines d'une réservation virtuelle est entièrement alloué, aucune autre machine virtuelle ne peut être provisionnée dans celle-ci. Les ressources peuvent être réservées au-delà de la capacité physique d'une ressource de calcul de virtualisation (engagement excessif), mais quand la capacité physique d'une ressource de calcul est allouée à 100 %, aucune autre machine ne peut être provisionnée sur aucune réservation avec cette ressource de calcul tant que les ressources sont récupérées.

- Si le Blueprint a des paramètres réseau spécifiques, la réservation doit disposer des mêmes réseaux.

Si le Blueprint ou la réservation spécifie un profil réseau pour l'attribution d'adresse IP statique, il est nécessaire qu'une adresse IP soit disponible pour l'attribuer à la nouvelle machine.

- Si le Blueprint ou la demande spécifie un emplacement, la ressource de calcul doit être associée à cet emplacement.

Si la valeur de la propriété personnalisée *VRM.Datacenter.Policy* est **Exact** qu'il n'existe aucune réservation d'une ressource de calcul associée à cet emplacement répondant à tous les autres critères, le provisionnement échoue.

Si la valeur de *VRM.Datacenter.Policy* est **NotExact** et qu'il n'existe aucune réservation pour une ressource de calcul associée à cet emplacement répondant à tous les autres critères, le provisionnement peut se poursuivre dans une autre réservation, quel que soit l'emplacement. Il s'agit de l'option par défaut.

- Si la Blueprint ou la demande spécifie la propriété personnalisée *VirtualMachine.Host.TpmEnabled*, le matériel approuvé doit être installé sur la ressource de calcul pour la réservation.
- Si le Blueprint spécifie une stratégie de réservation, la réservation doit faire partie de cette stratégie de réservation.

Les stratégies de réservation permettent de garantir que la réservation sélectionnée correspond aux conditions requises pour le provisionnement de machines avec un Blueprint spécifique. Par exemple, vous pouvez utiliser des stratégies de réservation pour limiter le provisionnement aux ressources de calcul avec un modèle spécifique pour le clonage.

Si aucune réservation répondant à tous les critères de sélection n'est disponible, le provisionnement échoue.

Si plusieurs réservations répondent à tous les critères, la réservation à partir de laquelle provisionner une machine demandée est déterminée par la logique suivante :

- une réservation avec une valeur de priorité inférieure est sélectionnée avant une réservation avec une valeur de priorité supérieure.
- Si plusieurs réservations ont la même priorité, la réservation avec le pourcentage de quota de machines alloué le plus bas est sélectionnée.
- Si plusieurs réservations ont une priorité et une utilisation de quota identiques, les machines sont distribuées parmi les réservations via le mécanisme Round-robin (répétition alternée).

Remarque Contrairement à la sélection Round-robin de profils réseau, la sélection Round-robin de réseaux (le cas échéant) est prise en charge et peut être associée à différents profils réseau.

Si plusieurs chemins de stockage sont disponibles sur une réservation avec une capacité suffisante pour provisionner les volumes de la machine, les chemins de stockage sont sélectionnés en fonction de la logique suivante :

- Si le Blueprint ou la demande spécifie une stratégie de réservation de stockage, le chemin de stockage doit faire partie de cette stratégie de réservation de stockage.

Si la valeur de la propriété personnalisée *VirtualMachine.DiskN.StorageReservationPolicyMode* est **NotExact** et qu'il n'y a aucun chemin de stockage avec suffisamment de capacité dans la stratégie de réservation de stockage, le provisionnement peut se poursuivre avec un chemin de stockage situé à l'extérieur de la stratégie de réservation de stockage spécifiée. La valeur par défaut de *VirtualMachine.DiskN.StorageReservationPolicyMode* est **Exact**.

- Un chemin de stockage avec une valeur de priorité inférieure est sélectionnée avant un chemin de stockage avec une valeur de priorité supérieure.
- Si plusieurs chemins de stockage ont une priorité identique, les machines sont distribuées parmi les chemins de stockage via le mécanisme Round-robin.

Création d'une réservation vSphere pour la virtualisation de réseau et de sécurité NSX

Vous pouvez utiliser une réservation vSphere pour attribuer des réseaux externes et des passerelles acheminées à des profils réseau pour les réseaux, spécifier la zone de transport et attribuer des groupes de sécurité aux composants de machine.

Si vous avez configuré NSX, vous pouvez spécifier la zone de transport NSX, la stratégie de réservation de passerelle Edge et acheminée, et les paramètres d'isolation d'application lorsque vous créez ou modifiez un Blueprint. Ces paramètres sont disponibles dans l'onglet **Paramètres NSX** sur les pages **Blueprint** et **Propriétés du Blueprint**.

Les paramètres du composant réseau et de sécurité que vous ajoutez au canevas de conception proviennent de votre configuration NSX et nécessitent l'exécution d'une collecte de données pour l'inventaire NSX pour les clusters vSphere. Les composants réseau et sécurité sont spécifiques à NSX et sont disponibles pour être utilisés avec des composants de machine vSphere uniquement. Pour plus d'informations sur la configuration de NSX, reportez-vous au *Guide d'administration de NSX*.

Lorsque vRealize Automation provisionne des machines avec la mise en réseau NAT ou acheminée, il provisionne une passerelle acheminée comme routeur réseau. La passerelle Edge ou acheminée est une machine de gestion qui consomme les ressources de calcul. Elle gère également les communications réseau des composants des machines provisionnées. La réservation utilisée pour provisionner la passerelle Edge ou acheminée détermine le réseau externe utilisé pour les profils de réseau NAT et acheminé. Elle détermine également la passerelle Edge ou acheminée de la réservation utilisée pour configurer les réseaux acheminés. La passerelle acheminée de la réservation relie les réseaux aux entrées dans la table de routage.

Vous pouvez spécifier une stratégie de réservation de la passerelle Edge ou acheminée afin d'identifier quelles réservations doivent être utilisées lors du provisionnement des machines en utilisant la passerelle Edge ou acheminée. Par défaut, vRealize Automation utilise les mêmes réservations pour la passerelle acheminée et pour les composants des machines.

Vous sélectionnez un ou plusieurs groupes de sécurité dans la réservation pour appliquer la stratégie de sécurité de base à toutes les machines des composants provisionnés avec cette réservation dans vRealize Automation. Chaque machine provisionnée est ajoutée à ces groupes de sécurité spécifiés.

Pour que le provisionnement réussisse, la zone de transport de la réservation doit correspondre à la zone de transport d'un Blueprint de machine lorsque ce Blueprint définit les réseaux des machines. De même, pour que le provisionnement de la passerelle acheminée d'une machine réussisse, la zone de transport définie dans la réservation doit correspondre à la zone de transport définie pour le Blueprint.

Lorsque vous sélectionnez une passerelle Edge ou acheminée et un profil réseau sur une réservation au moment de la configuration des réseaux acheminés, sélectionnez le chemin d'accès au réseau à utiliser en liant les réseaux acheminés ensemble et en l'attribuant au profil réseau externe utilisé pour configurer le profil réseau acheminé. La liste des profils réseau disponibles pour être attribués à un chemin réseau est filtrée pour correspondre au sous-réseau du chemin réseau basé sur le masque de sous-réseau et l'adresse IP principale sélectionnés pour l'interface réseau.

Si vous souhaitez utiliser une passerelle Edge ou acheminée dans des réservations vRealize Automation, configurez la passerelle acheminée de manière externe dans l'environnement NSX, puis exécutez une collecte de données d'inventaire. Pour NSX, vous devez disposer d'une instance de NSX Edge opérationnelle avant de pouvoir configurer la passerelle par défaut des itinéraires statiques ou les détails du routage dynamique d'une passerelle Edge Services Gateway ou d'un routeur Edge Distributed Router. Reportez-vous au guide d'administration de NSX.

Créer une réservation pour Hyper-V, KVM, SCVMM, vSphere ou XenServer

Vous devez attribuer des ressources aux machines en créant une réservation avant que les membres d'un groupe d'activité puissent demander le provisionnement des machines.

Chaque groupe d'activité doit avoir au moins une réservation pour ses membres afin de provisionner des machines de ce type. Par exemple, un groupe d'activité avec une réservation vSphere, mais pas une réservation KVM (RHEV), ne peuvent pas demander une machine virtuelle KVM (RHEV). Dans cet exemple, une réservation doit être allouée au groupe d'activité spécifiquement pour les ressources KVM (RHEV).

Procédure

1 Spécifiez les informations de réservation virtuelle

Chaque réservation est configurée pour un groupe d'activité spécifique afin d'octroyer aux utilisateurs l'accès aux machines demandées sur une ressource de calcul donnée.

2 Spécifier les ressources et les paramètres de mise en réseau pour une réservation virtuelle

Spécifiez les ressources et les paramètres réseau pour le provisionnement de machines à partir de cette réservation vRealize Automation.

3 Spécifier des propriétés personnalisées et des alertes pour les réservations virtuelles

Vous pouvez associer des propriétés personnalisées à une réservation vRealize Automation. Vous pouvez également configurer des alertes pour envoyer des notifications par e-mail lorsque les ressources de réservation sont faibles.

Spécifiez les informations de réservation virtuelle

Chaque réservation est configurée pour un groupe d'activité spécifique afin d'octroyer aux utilisateurs l'accès aux machines demandées sur une ressource de calcul donnée.

Vous pouvez contrôler l'affichage des réservations lors de leur ajout, de leur modification ou de leur suppression à l'aide de l'option **Filtrer par catégorie** de la page Réservations. Notez que les réservations d'agents de test n'apparaissent pas dans la liste de réservations lors d'un filtrage par catégorie.

Remarque Après avoir créé une réservation, vous ne pouvez pas modifier les associations de groupe d'activité ou de ressource de calcul.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur Fabric**.
- Vérifiez qu'un administrateur de locataire a créé au moins un groupe d'activité.
- Vérifiez qu'il existe une ressource de calcul.
- Configurez les paramètres réseau.
- (Facultatif) Configurez les informations sur le profil réseau.

Procédure

- 1 Sélectionnez **Infrastructure > Réservations > Réservations**.
- 2 Cliquez sur l'icône **Nouveau** (+) et sélectionnez le type de réservation que vous souhaitez créer.
Les types de réservation virtuelle disponibles sont Hyper-V, KVM, SCVMM, vSphere et XenServer.
Par exemple, sélectionnez **vSphere**.
- 3 (Facultatif) Sélectionnez une réservation existante dans le menu déroulant **Copier à partir d'une réservation existante**.
Les données de la réservation sélectionnée s'affichent. Vous pouvez apporter les modifications requises pour votre nouvelle réservation.
- 4 Entrez un nom dans la zone de texte **Nom**.
- 5 Sélectionnez un locataire dans le menu déroulant **Locataire**.
- 6 Sélectionnez un groupe d'activité dans le menu déroulant **Groupe d'activité**.
Seuls les utilisateurs de ce groupe d'activité peuvent provisionner des machines à l'aide de cette réservation.
- 7 (Facultatif) Sélectionnez une stratégie de réservation dans le menu déroulant **Stratégie de réservation**.
Cette option nécessite qu'il existe une ou plusieurs stratégies de réservation. Vous pouvez modifier la réservation ultérieurement afin de spécifier une stratégie de réservation.
Celle-ci vous permet de limiter le provisionnement à des réservations spécifiques.
- 8 Entrez un chiffre dans la zone de texte **Priorité** pour définir la priorité de la réservation.
La priorité est utilisée quand un groupe d'activité dispose de plusieurs réservations. Une réservation avec la priorité 1 est utilisée pour le provisionnement avant une réservation avec la priorité 2.

- 9 (Facultatif) Décochez la case **Activer cette réservation** si vous ne souhaitez pas que cette réservation soit active.

Ne quittez pas cette page. Votre réservation n'est pas terminée.

Spécifier les ressources et les paramètres de mise en réseau pour une réservation virtuelle

Spécifiez les ressources et les paramètres réseau pour le provisionnement de machines à partir de cette réservation vRealize Automation.

Vous pouvez sélectionner une banque de données FlexClone dans votre réservation si vous disposez d'un environnement vSphere et de périphériques de stockage s'appuyant sur la technologie Net App FlexClone. SDRS n'est pas pris en charge pour les périphériques de stockage FlexClone.

Pour réussir le provisionnement, la réservation doit disposer de suffisamment de stockage. La disponibilité de stockage de la réservation dépend des conditions suivantes :

- Quantité de stockage disponible sur la banque de données/cluster.
- Quantité de stockage réservée pour cette banque de données/cluster.
- Quantité de stockage déjà allouée dans vRealize Automation

Par exemple, même si l'instance de vCenter Server dispose de stockage pour la banque de données/cluster, si un stockage suffisant n'est pas réservé dans la réservation, le provisionnement échoue avec l'erreur « Aucune réservation n'est disponible pour l'allocation... ». Le stockage alloué sur une réservation dépend du nombre de machines virtuelles (quel que soit leur état) sur cette réservation spécifique. Consultez l'article de la base de connaissances VMware *Machine XXX : Aucune réservation n'est disponible à allouer au sein du groupe XXX. Un stockage total de XX Go a été demandé (2151030)* à l'adresse <http://kb.vmware.com/kb/2151030> pour plus d'informations.

Prérequis

Spécifiez les informations de réservation virtuelle.

Procédure

- 1 Cliquez sur l'onglet **Ressources**.
- 2 Sélectionnez une ressource de calcul sur laquelle provisionner des machines dans le menu déroulant **Ressource de calcul**.

Seuls les modèles situés sur le cluster que vous sélectionnez sont disponibles pour être clonés avec cette réservation.

Lors du provisionnement, les machines sont placées sur un hôte connecté au stockage local. Si la réservation utilise le stockage local, toutes les machines provisionnées par la réservation sont créées sur l'hôte qui contient ce stockage local. Cependant, si vous utilisez la propriété personnalisée `VirtualMachine.Admin.ForceHost`, qui force le provisionnement d'une machine sur un hôte différent, le provisionnement échoue. Le provisionnement échoue également si le modèle utilisé pour cloner la machine figure dans le stockage local, mais est associé à une machine appartenant à un autre cluster. Dans ce cas, l'échec est dû au fait que le provisionnement ne peut pas accéder au modèle.

- 3 (Facultatif) Entrez un chiffre dans la zone de texte **Quota de machines** pour définir le nombre maximal de machines pouvant être provisionnées dans cette réservation.

Seules les machines sous tension sont prises en compte dans le quota. Laissez cette zone vide pour rendre la réservation illimitée.

- 4 Spécifiez la quantité de mémoire, en Go, à allouer à cette réservation dans le tableau Mémoire.

La valeur de la mémoire globale de la réservation provient de la ressource de calcul que vous avez sélectionnée.

- 5 Sélectionnez un ou plusieurs chemins de stockage répertoriés.

Les options de chemins de stockage proviennent de la ressource de calcul que vous avez sélectionnée.

Pour les intégrations utilisant SDRS (Storage Distributed Resource Scheduler), vous pouvez sélectionner un cluster de stockage afin de permettre au SDRS de gérer automatiquement l'emplacement de stockage et l'équilibrage de charge des machines provisionnées dans cette réservation. Le mode Automatisation SDRS doit être défini sur Automatique. Sinon, sélectionnez une banque de données dans le cluster pour un comportement de banque de données autonome. SDRS n'est pas pris en charge pour les périphériques de stockage FlexClone.

Vous pouvez sélectionner des disques individuels du cluster ou un cluster de stockage, mais pas les deux. Si vous sélectionnez un cluster de stockage, SDRS contrôle le placement du stockage et l'équilibrage de charge pour les machines qui sont provisionnées depuis cette réservation.

- 6 Si disponible pour la ressource de calcul, sélectionnez un pool de ressources dans le menu déroulant **Pool de ressources**.
- 7 Cliquez sur l'onglet **Réseau**.

8 Configurez un chemin réseau pour les machines provisionnées à l'aide de cette réservation.

- a (Facultatif) Si l'option est disponible, sélectionnez un point de terminaison de stockage dans le menu déroulant **Point de terminaison**.

L'option FlexClone est visible dans la colonne des points de terminaison s'il existe un point de terminaison NetApp ONTAP et si l'hôte est virtuel. Si existe un point de terminaison NetApp ONTAP, la page de la réservation affiche le point de terminaison attribué au chemin de stockage. Lorsque vous ajoutez, mettez à jour ou supprimez un point de terminaison pour un chemin de stockage, la modification est visible dans toutes les réservations applicables.

Lorsque vous ajoutez, mettez à jour ou supprimez un point de terminaison pour un chemin de stockage, la modification est visible sur la page de la réservation.

- b Sélectionnez un chemin réseau pour les machines provisionnées par cette réservation dans la liste **Chemins d'accès au réseau**.

- c (Facultatif) Choisissez un profil réseau répertorié dans le menu déroulant **Profil réseau**.

Cette option nécessite qu'il existe un ou plusieurs profils réseau.

Vous pouvez sélectionner plusieurs chemins réseau sur une réservation, mais un seul réseau est utilisé lors du provisionnement d'une machine.

Vous pouvez à présent enregistrer la réservation en cliquant sur **Enregistrer**. Sinon, vous pouvez ajouter des propriétés personnalisées à d'autres spécifications de réservation du contrôle. Vous pouvez également configurer des alertes électroniques pour envoyer des notifications lorsque les ressources allouées à cette réservation deviennent faibles.

Spécifier des propriétés personnalisées et des alertes pour les réservations virtuelles

Vous pouvez associer des propriétés personnalisées à une réservation vRealize Automation. Vous pouvez également configurer des alertes pour envoyer des notifications par e-mail lorsque les ressources de réservation sont faibles.

Les propriétés personnalisées et les alertes électroniques sont des configurations facultatives de la réservation. Si vous ne souhaitez pas associer des propriétés personnalisées ou définir des alertes, cliquez sur **Enregistrer** pour terminer la création de la réservation.

Vous pouvez ajouter autant de propriétés personnalisées que vous le souhaitez.

Important Les notifications sont envoyées uniquement si des alertes électroniques sont configurées et que les notifications sont activées.

Si vous configurez des limites, les alertes sont générées tous les jours, plutôt que lorsque les seuils spécifiés sont atteints.

Prérequis

[Spécifier les ressources et les paramètres de mise en réseau pour une réservation virtuelle.](#)

Procédure

- 1 Cliquez sur l'onglet **Propriétés**.
- 2 Cliquez sur **Nouveau**.
- 3 Entrez un nom de propriété personnalisée valide.
- 4 Le cas échéant, entrez une valeur de propriété.
- 5 (Facultatif) Cochez la case **Chiffré** pour chiffrer la valeur de propriété.
- 6 (Facultatif) Cochez la case **Inviter l'utilisateur** pour demander à l'utilisateur d'entrer une valeur.
Cette option ne peut pas être remplacée lors du provisionnement.
- 7 (Facultatif) Ajoutez des propriétés personnalisées supplémentaires.
- 8 Cliquez sur l'onglet **Alertes**.
- 9 Cochez la case **Alertes de capacité** pour configurer les alertes à envoyer.
- 10 Utilisez le curseur pour définir des seuils pour l'allocation des ressources disponibles.
- 11 Entrez les noms d'utilisateurs ou de groupes Active Directory (et non les adresses e-mail) dans la zone de texte **Destinataires** pour recevoir des notifications d'alerte.
Entrez un nom sur chaque ligne. Appuyez sur Entrée pour séparer plusieurs entrées.
- 12 Sélectionnez **Envoyer des alertes au gestionnaire de groupes** pour inclure des gestionnaires de groupes aux alertes électroniques.
Les alertes par e-mail sont envoyés aux utilisateurs figurant dans la liste **Envoyer des e-mails du gestionnaire à** du groupe d'activité.
- 13 Spécifiez une fréquence de rappel (jours).
- 14 Cliquez sur **Enregistrer**.

La réservation est enregistrée et s'affiche dans la liste des Réservations.

Suivant

Vous pouvez configurer des stratégies de réservation facultatives ou commencer à préparer le provisionnement.

Les utilisateurs autorisés à créer des Blueprints peuvent les créer maintenant.

Modifier une réservation à attribuer à un profil réseau

Vous pouvez attribuer un profil réseau à une réservation, par exemple pour activer l'attribution des adresses IP statiques aux machines qui sont provisionnées sur cette réservation.

Vous pouvez également assigner un profil réseau à un Blueprint en utilisant la propriété personnalisée `VirtualMachine.NetworkN.ProfileName` sur l'onglet **Propriétés** de la page **Nouveau Blueprint** ou **Propriétés du Blueprint**.

Si vous spécifiez un profil réseau dans une réservation et un Blueprint, la valeur du Blueprint est prioritaire. Par exemple, si vous spécifiez un profil réseau dans le Blueprint à l'aide de la propriété personnalisée `VirtualMachine.NetworkN.ProfileName` et dans une réservation utilisée par le Blueprint, le profil réseau spécifié dans le Blueprint est prioritaire. Toutefois, si la propriété personnalisée n'est pas utilisée dans le Blueprint et que vous sélectionnez un profil réseau pour la carte réseau d'une machine, vRealize Automation utilise le chemin d'accès de réseau de réservation pour la carte réseau de la machine pour laquelle le profil réseau est spécifié.

Remarque Ces informations ne s'appliquent pas à Amazon Web Services.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur Fabric**.
- Créez un profil réseau. Reportez-vous à [Création d'un profil réseau](#).

Procédure

- 1 Sélectionnez **Infrastructure > Réservations > Réservations**.
- 2 Pointez vers une réservation et cliquez sur **Modifier**.
- 3 Cliquez sur l'onglet **Réseau**.
- 4 Attribuez un profil réseau à un chemin de réseau.
 - a Sélectionnez un chemin réseau sur lequel activer les adresses IP statiques.
Les options de chemin réseau sont dérivées des paramètres de l'onglet **Ressources**.
 - b Mappez un profil réseau disponible au chemin d'accès en sélectionnant un profil dans le menu déroulant **Profil réseau**.
 - c (Facultatif) Répétez cette étape pour attribuer des profils réseau à des chemins de réseau sur cette réservation.
- 5 Cliquez sur **OK**.

Stratégies de réservation

Vous pouvez utiliser une stratégie de réservation pour contrôler le traitement des demandes de réservation. Lorsque vous provisionnez des machines dans le Blueprint, le provisionnement est limité aux ressources spécifiées dans votre stratégie de réservation.

Les stratégies de réservation constituent un moyen facultatif de contrôler la manière dont les demandes de réservation sont traitées. Vous pouvez appliquer une stratégie de réservation à un Blueprint de manière à restreindre à un sous-ensemble des réservations disponibles les machines provisionnées à partir de ce Blueprint.

Vous pouvez utiliser une stratégie de réservation pour réunir dans des groupes des ressources de différents niveaux de service ou pour rendre facilement accessible un type spécifique de ressource à des fins particulières. Lorsqu'un utilisateur demande une machine, celle-ci peut être provisionnée sur n'importe quelle réservation de type approprié disposant d'une capacité suffisante pour cette machine. Les scénarios suivants offrent quelques exemples d'utilisations possibles des stratégies de réservation :

- Pour vous assurer que les machines provisionnées soient placées sur des réservations avec des périphériques spécifiques prenant en charge NetApp FlexClone.
- Pour limiter le provisionnement de machines de cloud à une région spécifique contenant une image de machine requise par un Blueprint spécifique.
- Comme moyen supplémentaire d'utiliser un modèle d'allocation de type Paiement à l'utilisation pour les types de machines prenant en charge cette capacité.

Vous pouvez ajouter plusieurs réservations à une stratégie de réservation, mais une réservation ne peut appartenir qu'à une seule stratégie. Vous pouvez attribuer une stratégie de réservation spécifique à plusieurs Blueprints. Un Blueprint ne peut avoir qu'une seule stratégie de réservation.

Remarque Les réservations définies pour les points de terminaison vCloud Air et vCloud Director ne prennent pas en charge l'utilisation de profils réseau pour le provisionnement des machines.

Remarque Si SDRS est activé sur votre plate-forme, vous pouvez permettre à SDRS d'équilibrer la charge de stockage de disques individuels d'une machine virtuelle ou de l'ensemble du stockage de la machine virtuelle. Si vous travaillez avec des clusters de banques de données SDRS, des conflits peuvent survenir lorsque vous utilisez des stratégies de réservation et des stratégies de réservation de stockage. Par exemple, si une banque de données autonome ou une banque de données au sein d'un cluster SDRS est sélectionnée sur l'une des réservations d'une stratégie ou d'une stratégie de stockage, le stockage de votre machine virtuelle pourrait être figé plutôt que piloté par SDRS. Si vous demandez le provisionnement d'une machine avec un placement de stockage sur un cluster SDRS, la machine est supprimée si le niveau d'automatisation SDRS est désactivé.

Configurer une stratégie de réservation

Vous pouvez créer des stratégies de réservation pour collecter des ressources en groupes pour différents niveaux de service ou pour rendre facilement accessible un type spécifique de ressource à des fins particulières. Après avoir créé la stratégie de réservation, vous devez ensuite la renseigner avec les réservations avant que les administrateurs de locataire et les gestionnaires des groupes d'activité puissent utiliser la stratégie dans un Blueprint de façon efficace.

Une stratégie de réservation peut inclure des réservations de différents types, mais seules les réservations correspondant au type de Blueprint sont prises en considération lors de la sélection d'une réservation dans le cadre d'une demande particulière.

Procédure

1 Créer une stratégie de réservation

Vous pouvez utiliser des stratégies de réservation pour regrouper des réservations similaires.

2 Attribuer une stratégie de réservation à une réservation

Vous pouvez attribuer une stratégie de réservation à une réservation lorsque vous créez la réservation. Vous pouvez également modifier une réservation existante afin de lui attribuer une stratégie de réservation ou modifier son attribution de stratégie de réservation.

Créer une stratégie de réservation

Vous pouvez utiliser des stratégies de réservation pour regrouper des réservations similaires.

Créer la stratégie de réservation en premier, puis ajoutez la stratégie aux réservations pour permettre à l'auteur d'un Blueprint d'utiliser la stratégie de réservation dans un Blueprint.

La stratégie est créée comme un conteneur vide.

Vous pouvez contrôler l'affichage des stratégies de réservation lors de leur ajout, de leur modification ou de leur suppression à l'aide de l'option **Filtrer par type** de la page Stratégies de réservation.

Prérequis

Connectez-vous à la console de vRealize Automation en tant qu'**administrateur Fabric**.

Procédure

- 1 Sélectionnez **Infrastructure > Réservations > Stratégies de réservation**.
- 2 Cliquez sur **Ajouter**.
- 3 Entrez un nom dans la zone de texte **Nom**.
- 4 Sélectionnez une **Stratégie de réservation** dans le menu déroulant **Type**.
- 5 Entrez une description dans la zone de texte **Description**.
- 6 Cliquez sur **Mettre à jour** pour enregistrer la stratégie.

Attribuer une stratégie de réservation à une réservation

Vous pouvez attribuer une stratégie de réservation à une réservation lorsque vous créez la réservation. Vous pouvez également modifier une réservation existante afin de lui attribuer une stratégie de réservation ou modifier son attribution de stratégie de réservation.

Prérequis

[Créer une stratégie de réservation](#).

Procédure

- 1 Sélectionnez **Infrastructure > Réservations > Réservations**.
- 2 Pointez vers une réservation et cliquez sur **Modifier**.
- 3 Sélectionnez une stratégie de réservation dans le menu déroulant **Stratégie de réservation**.
- 4 Cliquez sur **Enregistrer**.

Stratégies de réservation de stockage

Vous pouvez créer des stratégies de réservation de stockage visant à autoriser les architectes de Blueprint à attribuer les volumes d'une machine virtuelle à différentes banques de données pour les types de plate-forme vSphere, KVM (RHEV) et SCVMM ou différents profils de stockage pour d'autres ressources, par exemple des ressources vCloud Air ou vCloud Director.

L'attribution des volumes à une machine virtuelle à différentes banques de données ou à un profil de stockage différent autorise les architectes de Blueprint à contrôler et à utiliser l'espace de stockage de manière plus efficace. Par exemple, ils peuvent déployer le volume du système d'exploitation sur une banque de données ou un profil de stockage plus lent et moins onéreux, et le volume de base de données sur une banque de données ou un profil de stockage plus rapide.

Certains points de terminaison de machine ne prennent en charge qu'un seul profil de stockage, tandis que d'autres prennent en charge un stockage sur disque à plusieurs niveaux. Le stockage sur disque à plusieurs niveaux est disponible pour les points de terminaison vCloud Director 5.6 et versions ultérieures, ainsi que pour les points de terminaison vCloud Air. Le stockage sur disque à plusieurs niveaux n'est pas pris en charge pour les points de terminaison vCloud Director 5.5.

Lorsque vous créez un Blueprint, vous pouvez attribuer une banque de données unique ou une stratégie de réservation de stockage qui représente plusieurs banques de données sur un volume. Lorsqu'ils attribuent une banque de données ou un profil de stockage unique à un volume, vRealize Automation l'utilise, si possible, au moment du provisionnement. Lorsqu'ils attribuent une stratégie de réservation de stockage à un volume, vRealize Automation utilise l'une de ses banques de données ou l'un de ses profils de stockage s'ils utilisent d'autres ressources, comme vCloud Air ou vCloud Director au moment du provisionnement.

Une stratégie de réservation de stockage est essentiellement une balise appliquée à une ou plusieurs banques de données ou à un ou plusieurs profils de stockage par un administrateur Fabric à des groupes de banques de données ou de profils de stockage ayant des caractéristiques similaires, comme la vitesse ou le coût. Une banque de données ou un profil de stockage peut être attribué à une seule stratégie de réservation de stockage à la fois, mais une stratégie de réservation de stockage peut avoir plusieurs banques de données différentes ou plusieurs profils de stockage différents.

Vous pouvez créer une stratégie de réservation de stockage et l'attribuer à une ou plusieurs banques de données ou à un ou plusieurs profils de stockage. L'auteur d'un Blueprint peut ensuite attribuer la stratégie de réservation de stockage à un volume dans un Blueprint virtuel. Lorsqu'un utilisateur demande une machine qui utilise le Blueprint, vRealize Automation utilise la stratégie de réservation de stockage spécifiée dans le Blueprint pour sélectionner une banque de données ou un profil de stockage pour le volume de la machine.

Remarque Si SDRS est activé sur votre plate-forme, vous pouvez permettre à SDRS d'équilibrer la charge de stockage de disques individuels d'une machine virtuelle ou de l'ensemble du stockage de la machine virtuelle. Si vous travaillez avec des clusters de banques de données SDRS, des conflits peuvent survenir lorsque vous utilisez des stratégies de réservation et des stratégies de réservation de stockage. Par exemple, si une banque de données autonome ou une banque de données au sein d'un cluster SDRS est sélectionnée sur l'une des réservations d'une stratégie ou d'une stratégie de stockage, le stockage de votre machine virtuelle pourrait être figé plutôt que piloté par SDRS. Si vous demandez le provisionnement d'une machine avec un placement de stockage sur un cluster SDRS, la machine est supprimée si le niveau d'automatisation SDRS est désactivé.

Le stockage et la mémoire alloués à une machine provisionnée via une réservation sont libérés lorsque la machine est supprimée dans vRealize Automation par l'action Détruire. Le stockage et la mémoire ne sont pas libérés si la machine est supprimée dans vCenter Server.

Par exemple, vous ne pouvez pas supprimer une réservation associée aux machines d'un déploiement existant. Si vous déplacez ou supprimez des machines déployées manuellement dans vCenter Server, vRealize Automation continue de reconnaître les machines déployées comme étant en temps réel et vous empêche de supprimer les réservations associées.

Configurer une stratégie de réservation de stockage

Vous pouvez créer des stratégies de réservation de stockage pour grouper des banques de données ayant des caractéristiques similaires, comme la vitesse ou le prix. Après avoir créé la stratégie de réservation de stockage, vous devez la renseigner avec les banques de données avant d'utiliser la stratégie dans un Blueprint.

Procédure

1 Créer une stratégie de réservation de stockage

Vous pouvez utiliser une stratégie de réservation de stockage pour grouper des banques de données ayant des caractéristiques similaires, comme la vitesse ou le prix.

2 Attribuer une stratégie de réservation de stockage à une banque de données

Vous pouvez associer une stratégie de réservation de stockage à une ressource de calcul. Une fois la stratégie de réservation de stockage créée, renseignez-la avec les banques de données. Une banque de données ne peut appartenir qu'à une seule stratégie de réservation de stockage. Ajoutez plusieurs banques de données pour créer un groupe de banques de données à utiliser avec un Blueprint.

Créer une stratégie de réservation de stockage

Vous pouvez utiliser une stratégie de réservation de stockage pour grouper des banques de données ayant des caractéristiques similaires, comme la vitesse ou le prix.

La stratégie est créée comme un conteneur vide.

Vous pouvez contrôler l'affichage des stratégies de réservation lors de leur ajout, de leur modification ou de leur suppression à l'aide de l'option **Filtrer par type** de la page Stratégies de réservation.

Prérequis

Connectez-vous à la console de vRealize Automation en tant qu'**administrateur Fabric**.

Procédure

- 1 Sélectionnez **Infrastructure > Réservations > Stratégies de réservation**.
- 2 Cliquez sur **Ajouter**.
- 3 Entrez un nom dans la zone de texte **Nom**.
- 4 Sélectionnez une **Stratégie de réservation de stockage** dans le menu déroulant **Type**.
- 5 Entrez une description dans la zone de texte **Description**.
- 6 Cliquez sur **Mettre à jour** pour enregistrer la stratégie.

Attribuer une stratégie de réservation de stockage à une banque de données

Vous pouvez associer une stratégie de réservation de stockage à une ressource de calcul. Une fois la stratégie de réservation de stockage créée, renseignez-la avec les banques de données. Une banque de données ne peut appartenir qu'à une seule stratégie de réservation de stockage. Ajoutez plusieurs banques de données pour créer un groupe de banques de données à utiliser avec un Blueprint.

Prérequis

[Créer une stratégie de réservation de stockage.](#)

Procédure

- 1 Sélectionnez **Infrastructure > Ressources de calcul > Ressources de calcul**.
- 2 Pointez vers une ressource de calcul et cliquez sur **Modifier**.
- 3 Cliquez sur l'onglet **Configuration**.
- 4 Localisez la banque de données à ajouter à votre stratégie de réservation de stockage dans le tableau Stockage.
- 5 Cliquez sur l'icône **Modifier** (✎) en regard de l'objet **Chemin de stockage** souhaité.
- 6 Sélectionnez une stratégie de réservation de stockage dans le menu déroulant de la colonne **Stratégie de réservation de stockage**.

Après avoir provisionné une machine, vous ne pouvez pas modifier sa stratégie de réservation de stockage. Le cas échéant, vous modifieriez également le profil de stockage sur disque.

- 7 Cliquez sur l'icône **Enregistrer** (✓).
- 8 Cliquez sur **OK**.
- 9 (Facultatif) Attribuer des banques de données supplémentaires à votre stratégie de réservation de stockage.

positionnement de la charge de travail

Lorsque vous déployez un Blueprint, le positionnement de la charge de travail utilise les données collectées pour justifier à quel endroit déployer le Blueprint en fonction des ressources disponibles. vRealize Automation et vRealize Operations Manager fonctionnent ensemble afin de fournir des recommandations de positionnement pour les charges de travail dans le déploiement de nouveaux Blueprints.

Alors que vRealize Automation gère des stratégies d'entreprise, tels que les groupes d'activité, les réservations et les quotas, il s'intègre aux analyses de capacité de vRealize Operations Manager pour placer les machines. Le positionnement de la charge de travail est disponible uniquement pour les points de terminaison vSphere.

Termes de positionnement de la charge de travail utilisés

Plusieurs termes sont utilisés en rapport avec le positionnement de la charge de travail.

- Dans vSphere, les clusters établissent des mappages vers les ressources de calcul de vRealize Automation.
- Les réservations incluent le calcul et le stockage, et le stockage peut être composé de banques de données individuelles ou de clusters de banque de données. Une réservation peut inclure plusieurs banques de données, des clusters de banques de données ou les deux.
- Plusieurs réservations peuvent désigner le même cluster.
- Des machines virtuelles peuvent se déplacer sur plusieurs clusters.
- Lorsque le positionnement de la charge de travail est activé, le workflow de provisionnement utilise la stratégie de positionnement pour justifier à quel endroit déployer le Blueprint.

Provisionnement de Blueprints avec le positionnement de la charge de travail

Lorsque vous utilisez le positionnement de la charge de travail pour provisionner des Blueprints, le workflow de provisionnement utilise les réservations de vRealize Automation et l'optimisation de positionnement depuis vRealize Operations Manager.

- 1 vRealize Automation fournit des règles de gouvernance pour autoriser les destinations de positionnement.
- 2 vRealize Operations Manager fournit des recommandations pour l'optimisation du positionnement en fonction de données analytiques.
- 3 vRealize Automation continue le processus de provisionnement en suivant les recommandations de positionnement depuis vRealize Operations Manager.

Si vRealize Operations Manager ne peut pas fournir une recommandation, ou si la recommandation ne peut pas être utilisée, vRealize Automation revient à sa logique de positionnement par défaut.

Lorsqu'un développeur sélectionne un élément du catalogue et complète le formulaire de demande d'élément de catalogue, vRealize Automation prend en compte les considérations suivantes pour le provisionnement des machines virtuelles.

Tableau 2-16. Considérations relatives au provisionnement de machines virtuelles

Élément à prendre en compte	Effet
Stratégies	La stratégie de réservation vRealize Automation peut indiquer plusieurs réservations.
Réservations	<p>vRealize Automation évalue la demande et détermine quelles réservations peuvent satisfaire les contraintes spécifiées dans la demande.</p> <ul style="list-style-type: none"> ■ Si le positionnement est activé et basé sur les analyses de vRealize Operations Manager, vRealize Automation transmet la liste des réservations à vRealize Operations Manager afin de déterminer la réservation la mieux adaptée au positionnement en fonction de mesures opérationnelles. ■ Si le positionnement n'est pas basé sur vRealize Operations Manager, vRealize Automation décide du positionnement en fonction des priorités et de la disponibilité. <p>Les réservations sont mises à jour pour effectuer le suivi de la consommation des ressources.</p> <p>Si vRealize Operations Manager recommande un cluster ou une banque de données que vRealize Automation considère comme non applicable ou ne répondant plus aux exigences de capacité, vRealize Automation enregistre l'exception. vRealize Automation permet au provisionnement de se poursuivre en fonction de ses mécanismes de positionnement par défaut.</p>

Pour identifier les ressources pour une machine virtuelle, vRealize Automation fournit une liste de réservations de candidats. Chaque candidat de la liste peut inclure un cluster et un ou plusieurs banques de données ou clusters de banque de données. vRealize Operations Manager utilise les réservations de candidats pour créer la liste de candidats de destination et localiser la meilleure cible.

La stratégie de vRealize Operations Manager définit le niveau d'équilibre, l'utilisation et l'espace de mémoire tampon pour le cluster. Pour une réservation spécifique, qui est en fait un cluster ou un cluster de banque de données, vRealize Automation vérifie si la recommandation est une destination de positionnement viable.

- Si la destination est viable, vRealize Automation déploie le Blueprint en fonction de la recommandation.
- Si la destination n'est pas viable, vRealize Automation utilise le comportement de positionnement par défaut pour placer les machines virtuelles.

Les considérations relatives au positionnement doivent également tenir compte des problèmes de santé et d'utilisation. Alors que l'administrateur de cloud et l'administrateur d'infrastructure virtuelle gèrent l'infrastructure, les développeurs s'intéressent à la santé de leurs applications. Pour aider les développeurs, la stratégie de positionnement de la charge de travail doit également tenir compte des problèmes de santé et d'utilisation.

Tableau 2-17. Considérations relatives à la santé et problèmes d'utilisation

Problème lié à la charge de travail	Solution de positionnement
Un développeur remarque un problème de santé dans l'environnement.	vRealize Automation provisionne les Blueprints dans les clusters qui rencontrent des problèmes ou qui sont trop utilisés en raison de charges de travail trop importantes. vRealize Automation doit intégrer les analyses de capacité dans vRealize Operations Manager pour assurer que les Blueprints soient provisionnés dans des clusters ayant une capacité suffisante.
Un développeur remarque un problème d'utilisation.	Les clusters de l'environnement sont sous-utilisés. vRealize Automation doit s'intégrer aux analyses de capacité fournies par vRealize Operations Manager pour s'assurer que les Blueprints sont provisionnés dans un cluster dans lequel l'utilisation est maximisée.

Utilisateurs de provisionnement de Blueprints

Les utilisateurs suivants effectuent des actions pour provisionner des Blueprints.

Tableau 2-18. Utilisateurs et rôles de provisionnement de Blueprints

Étape	Utilisateur	Action	Rôle requis
1	Administrateur de cloud ou administrateur d'infrastructure virtuelle (VI)	S'assure que le positionnement initial des machines virtuelles répond aux stratégies d'organisation et qu'elles sont optimisées selon les données analytiques opérationnelles.	Rôle d'administrateur IaaS
1	Administrateur Fabric	Définit les réservations, les stratégies de réservation et la stratégie de positionnement dans vRealize Automation.	Rôle d'administrateur Fabric, d'architecte d'infrastructure
1	Administrateur IaaS	Définit les points de terminaison pour vSphere et vRealize Operations Manager qui sont nécessaires pour le positionnement de la charge de travail.	Rôle d'administrateur IaaS
2	Architecte d'infrastructure	En tant qu'architecte de Blueprint qui travaille directement avec les types de composants de machine virtuelle, attribue les stratégies de réservation aux machines virtuelles lors de la création d'un Blueprint. Spécifie la stratégie de réservation en tant que propriété du composant de machine dans le Blueprint.	Architecte d'infrastructure

Tableau 2-18. Utilisateurs et rôles de provisionnement de Blueprints (suite)

Étape	Utilisateur	Action	Rôle requis
3	Architecte d'infrastructure, architecte d'application, architecte de logiciel et architecte XaaS	<p>Crée et publie le Blueprint pour provisionner les machines virtuelles. Seul l'architecte d'infrastructure travaille directement avec les composants de machine. Les autres rôles d'architecte peuvent réutiliser des Blueprints d'infrastructure dans l'imbrication, mais ils ne peuvent pas modifier les paramètres de composant de machine.</p> <p>Le Blueprint peut inclure un composant unique ou il peut inclure des Blueprints imbriqués, des composants XaaS, plusieurs machines virtuelles dans une application multiniveau, etc.</p> <p>vRealize Automation positionne les machines virtuelles en fonction de la configuration des réservations et, éventuellement, inclut la stratégie de réservation au niveau du composant de machine pour le Blueprint. Par exemple, votre Blueprint peut inclure deux machines, une stratégie différente étant appliquée à chaque machine.</p> <p>vRealize Automation optimise également les machines virtuelles selon les données analytiques opérationnelles fournies par vRealize Operations Manager.</p>	Architecte d'infrastructure
4	Administrateur de cloud ou administrateur VI	<p>Sélectionne les stratégies qui régissent le positionnement initial des machines virtuelles provisionnées par vRealize Automation.</p> <p>L'administrateur de Cloud peut :</p> <ul style="list-style-type: none"> ■ Sélectionner les stratégies à l'aide d'une API. ■ Utiliser la stratégie de positionnement par défaut, qui utilise chaque serveur vRealize Automation à son tour pour équilibrer les charges de travail. Cette approche ne nécessite pas d'entrée provenant de vRealize Operations Manager. 	Rôle d'administrateur IaaS, architecte d'infrastructure
5	Administrateur VI	Génère le centre de données personnalisé et les groupes personnalisés dans vRealize Operations Manager. Ensuite, l'administrateur VI applique la stratégie utilisée pour consolider et équilibrer les charges de travail aux centres de données personnalisés.	Rôle d'administrateur IaaS, architecte d'infrastructure
6	Administrateur Fabric	<p>Sélectionne la stratégie de positionnement dans vRealize Automation.</p> <p>Utiliser la stratégie de positionnement de la charge de travail pour que vRealize Automation détermine où placer les machines lorsque vous déployez de nouveaux Blueprints. La stratégie de positionnement requiert une entrée de vRealize Operations Manager</p>	Rôle d'administrateur Fabric

Tableau 2-18. Utilisateurs et rôles de provisionnement de Blueprints (suite)

Étape	Utilisateur	Action	Rôle requis
7	Développeur	Demande un Blueprint pour provisionner des machines virtuelles. Le Blueprint peut être composé de plusieurs machines pour exécuter une application à trois niveaux.	
8	Développeur	Lorsque le développeur déploie le Blueprint, vRealize Operations Manager recherche une stratégie de positionnement correspondant aux clusters appropriés pour la demande.	

Pour plus d'informations sur la stratégie de positionnement, reportez-vous à [Stratégie de positionnement](#).

Pour configurer le positionnement de la charge de travail, reportez-vous à la section [Configuration d'un positionnement de la charge de travail](#).

Distributed Resource Scheduler (DRS) est requis pour positionner les machines virtuelles

vSphere DRS est le moteur de positionnement que vRealize Automation et vRealize Operations Manager utilisent pour provisionner et placer les machines virtuelles.

Pour que vRealize Automation suggère le meilleur positionnement pour les machines virtuelles, vous devez activer DRS sur le cluster et le rendre entièrement automatisé. vRealize Automation utilise alors les API de vSphere DRS pour déterminer le positionnement approprié des machines virtuelles.

vRealize Automation s'intègre au service de positionnement de vRealize Operations Manager. vRealize Operations Manager fournit uniquement les recommandations de positionnement pour les clusters sur lesquels DRS est activé et entièrement automatisé.

Limitations pour le positionnement de la charge de travail

Lorsque vous utilisez la stratégie de positionnement relative au positionnement de la charge de travail pour placer les machines lorsque vous déployez de nouveaux Blueprints, vous devez connaître les limitations.

- Dans vRealize Operations Manager, la solution vRealize Automation identifie les clusters et les machines virtuelles gérés par vRealize Automation.
- Lorsque vRealize Automation gère les objets enfants d'un centre de données ou un conteneur de centre de données personnalisé dans vRealize Operations Manager, la capacité à rééquilibrer ou à déplacer ces objets n'est pas disponible. Vous ne pouvez pas activer ou désactiver l'exclusion des actions sur les objets gérés de vRealize Automation .
- Pour les objets gérés par vRealize Automation, le comportement de positionnement de la charge de travail est le suivant :
 - Lorsqu'un centre de données personnalisé ou un centre de données comprend un cluster géré par vRealize Automation, le positionnement de la charge de travail ne vous permet pas de rééquilibrer le cluster.
 - Quand un cluster inclut des machines virtuelles gérées par vRealize Automation, le positionnement de la charge de travail ne vous permet pas de déplacer ces machines virtuelles.

- vRealize Operations Manager ne prend pas en charge le positionnement de la charge de travail sur des pools de ressources dans vCenter Server.
- vRealize Operations Manager ne prend pas en charge vSAN dans la version actuelle.

Autorisations de configuration du positionnement de la charge de travail

Vous devez disposer d'autorisations dans vRealize Automation et vRealize Operations Manager pour configurer le positionnement de la charge de travail et la stratégie de positionnement.

Dans vRealize Automation, vous devez avoir le rôle d'administrateur Fabric pour configurer le positionnement de la charge de travail. Reportez-vous à présentation de rôles d'utilisateur dans le Centre d'informations vRealize Automation.

Dans vRealize Operations Manager, vous devez créer un rôle d'utilisateur pour le positionnement de la charge de travail et attribuer des autorisations au rôle.

- Sur le compte d'utilisateur, attribuez l'autorisation en lecture seule aux hôtes et clusters vSphere et au stockage vSphere dans la hiérarchie d'objets.
- Pour que le rôle d'utilisateur puisse utiliser des appels d'API dans le positionnement de la charge de travail, attribuez des autorisations d'accès en lecture et en écriture sur les API. Sélectionnez **Administration > Contrôle d'accès > Autorisations**, puis sélectionnez **API REST > Tous les autres lecture, écriture sur les API**.

vRealize Automation utilise le rôle vRealize Operations Manager lorsque vous enregistrez le point de terminaison et pour demander des recommandations de positionnement lors du provisionnement pour le compte des utilisateurs qui demandent des éléments du catalogue.

Pour plus d'informations, reportez-vous à la section Contrôle d'accès dans le Centre d'informations vRealize Operations Manager.

Stratégie de positionnement

Vous pouvez utiliser la stratégie de positionnement pour que vRealize Automation détermine où placer les machines lorsque vous déployez de nouveaux Blueprints. La stratégie de positionnement utilise les analyses de vRealize Operations Manager pour identifier les charges de travail sur vos clusters afin qu'elle puisse proposer des destinations de positionnement.

Vous devez effectuer plusieurs étapes avant de pouvoir utiliser la stratégie de positionnement. Dans vRealize Automation, vous créez des points de terminaison pour les instances de vRealize Operations Manager et de vCenter Server. Ensuite, vous créez un groupe fabric et ajoutez des réservations pour votre point de terminaison vCenter Server.

Pour garantir que vRealize Operations Manager fournit une analyse de positionnement de la charge de travail à vRealize Automation, vous devez :

- Installer la solution vRealize Automation dans l'instance de vRealize Operations Manager qui est utilisée pour le positionnement de la charge de travail.
- Configurer vRealize Operations Manager pour surveiller le système vCenter Server.

Pour configurer vRealize Automation et vRealize Operations Manager pour le positionnement de la charge de travail, reportez-vous à la section [Configuration d'un positionnement de la charge de travail](#).

Localisation de la stratégie de positionnement

Dans votre instance de vRealize Automation, sélectionnez **Infrastructure > Réservations > Stratégie de positionnement**.

Pour utiliser l'analyse de positionnement de la charge de travail fournie par vRealize Operations Manager, sélectionnez **Utiliser vRealize Operations Manager pour les recommandations de positionnement**.

Si vous n'utilisez pas la stratégie de positionnement de la charge de travail, vRealize Automation utilise la méthode de positionnement par défaut.

Configuration d'un positionnement de la charge de travail

Pour utiliser la stratégie de positionnement afin de positionner des machines lorsque vous déployez de nouveaux Blueprints, vous devez configurer vRealize Automation de façon à utiliser les analyses fournies par vRealize Operations Manager. Vous pouvez également configurer vRealize Operations Manager afin d'appliquer une stratégie destinée à consolider et équilibrer les charges de travail par rapport aux ressources de calcul de votre cluster.

Dans vRealize Automation, vous configurez des points de terminaison, créez un groupe Fabric et ajoutez des réservations. Dans vRealize Operations Manager, vous pouvez configurer une stratégie pour prendre en charge l'équilibrage de charge de travail et appliquer cette stratégie à un groupe personnalisé qui inclut vos ressources de calcul personnalisées.

Prérequis

Pour que la stratégie de positionnement puisse proposer des destinations de positionnement pour les Blueprints, vous devez préalablement effectuer plusieurs étapes.

- Assimilez la stratégie de positionnement. Reportez-vous à [Stratégie de positionnement](#).
- Assurez-vous qu'il existe un point de terminaison dans vRealize Automation pour l'instance de vRealize Operations Manager utilisée pour le positionnement de la charge de travail. Reportez-vous à [Créer un point de terminaison vRealize Operations Manager](#).
- Assurez-vous qu'il existe un point de terminaison dans vRealize Automation pour l'instance de vCenter Server. Reportez-vous à [Créer un point de terminaison vSphere](#).
- Ajoutez des réservations au point de terminaison vCenter Server. Reportez-vous à [Réservations](#).
- Ajoutez un groupe Fabric et assurez-vous que votre utilisateur est un administrateur de groupe Fabric. Reportez-vous à [Créer un groupe Fabric](#).
- Vérifiez que vRealize Operations Manager surveille la même infrastructure que celle surveillée par vRealize Automation pour vous assurer qu'elles incluent les mêmes instances de vCenter Server. Reportez-vous à la section [Solution VMware vSphere dans vRealize Operations Manager](#) dans le centre d'informations de vRealize Operations Manager.

- Assimilez les concepts de réservations, réservation de stockage, Blueprints et fournisseurs de délégation. Reportez-vous au Centre d'informations de vRealize Automation.
- Assimilez et définissez les paramètres de remplissage et d'équilibre dans la stratégie de vRealize Operations Manager utilisée pour le positionnement de la charge de travail. Reportez-vous à la section [Détails d'automatisation de charge de travail](#) dans le centre d'informations de vRealize Operations Manager.

Procédure

1 [Configurer vRealize Automation pour le positionnement de la charge de travail](#)

Pour utiliser l'analyse de positionnement de la charge de travail afin de placer les machines lorsque vous déployez de nouveaux blueprints, vous devez préparer l'instance de vRealize Automation.

2 [Configurer vRealize Operations Manager pour le positionnement de la charge de travail dans vRealize Automation](#)

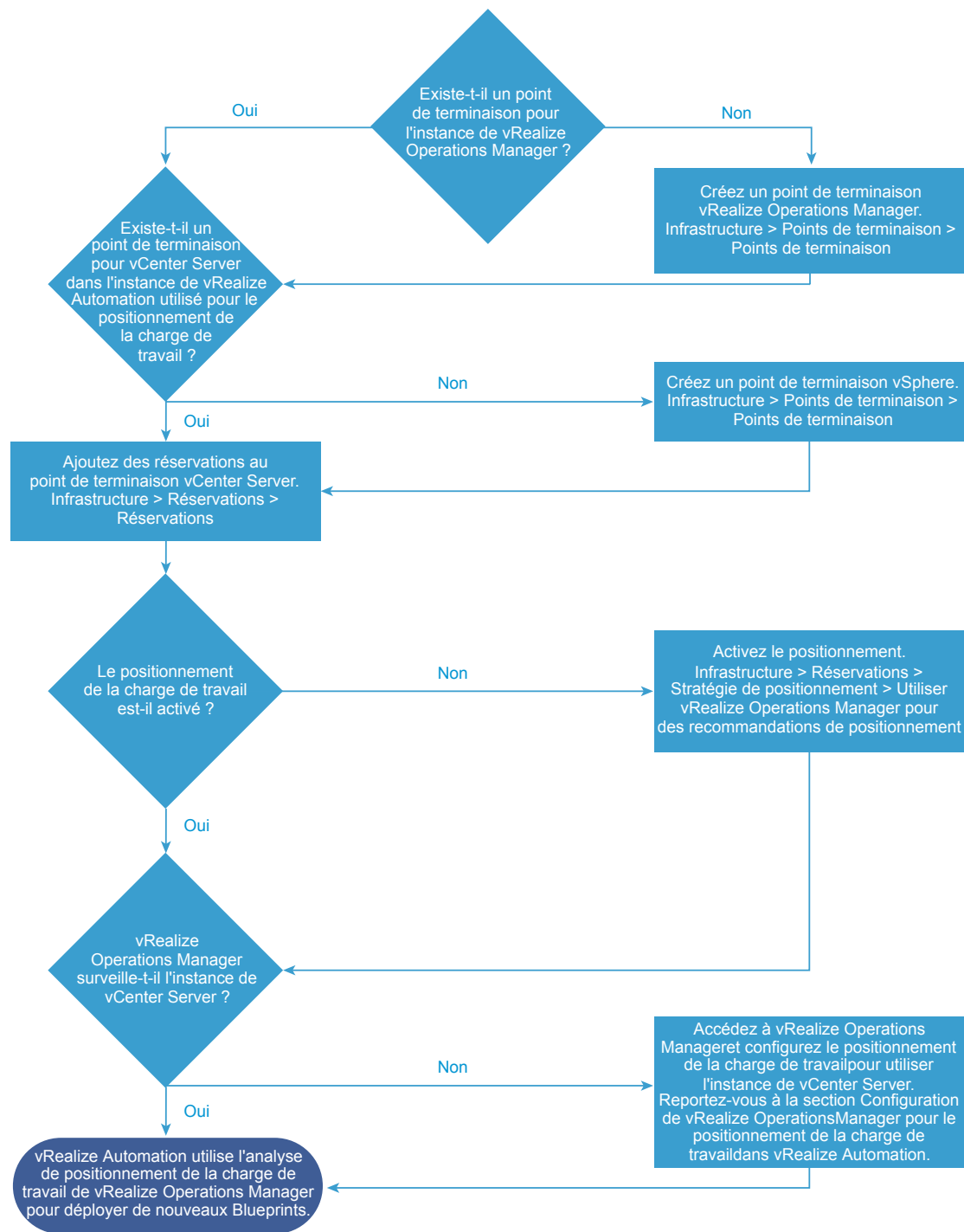
Pour fournir l'analyse de positionnement de la charge de travail à vRealize Automation afin de placer les machines lorsque vous déployez de nouveaux blueprints, vous devez préparer l'instance de vRealize Operations Manager.

Vous avez configuré vRealize Automation et vRealize Operations Manager pour utiliser les analyses du positionnement de la charge de travail afin de proposer des destinations de positionnement pour les nouveaux Blueprints.

Configurer vRealize Automation pour le positionnement de la charge de travail

Pour utiliser l'analyse de positionnement de la charge de travail afin de placer les machines lorsque vous déployez de nouveaux blueprints, vous devez préparer l'instance de vRealize Automation.

Pour préparer votre instance de vRealize Automation en vue de l'utilisation de la stratégie de positionnement, vous configurez des points de terminaison, créez un groupe Fabric et ajoutez des réservations.



Prérequis

- Pour utiliser le positionnement de la charge de travail, vous devez connaître les conditions requises. Reportez-vous à [Configuration d'un positionnement de la charge de travail](#).
- Dans vRealize Automation, ajoutez un rôle d'utilisateur spécifique et des autorisations pour vRealize Operations Manager afin de valider les informations d'identification. Reportez-vous à présentation de rôles d'utilisateur dans le Centre d'informations vRealize Automation.

Procédure

- 1 Dans votre instance de vRealize Automation, ajoutez un point de terminaison pour l'instance de vRealize Operations Manager et cliquez sur **OK**.
 - a Sélectionnez **Infrastructure > Point de terminaison > Points de terminaison**.
 - b Sélectionnez **Nouveau > Gestion > vRealize Operations Manager**.
 - c Entrez les informations générales pour le point de terminaison **vRealize Operations Manager**.

Vous n'avez pas besoin de spécifier les propriétés pour le point de terminaison.

- 2 Dans votre instance de vRealize Automation, ajoutez un point de terminaison pour l'instance de vCenter Server et cliquez sur **OK**.
 - a Sélectionnez **Infrastructure > Point de terminaison > Points de terminaison**.
 - b Sélectionnez **Nouveau > Virtuel > vSphere (vCenter)**.
 - c Entrez les informations générales, les propriétés et les associations pour le point de terminaison vCenter Server.

Une fois que vous avez ajouté des points de terminaison, et que vRealize Automation a collecté des données à partir de ceux-ci, les ressources de calcul pour ces points de terminaison sont disponibles. Vous pouvez ensuite ajouter ces ressources de calcul au groupe Fabric que vous créez.

- 3 Créez un groupe Fabric afin que les autres utilisateurs puissent créer des réservations et activer la stratégie de positionnement.
 - a Sélectionnez **Infrastructure > Point de terminaison > Groupes Fabric**.
 - b Cliquez sur **Nouveau** et entrez les informations sur le groupe Fabric.

Option	Description
Nom	Entrez un nom significatif pour le groupe Fabric.
Description	Entrez une description utile.
Administrateurs Fabric	Entrez l'adresse e-mail de chaque personne à désigner comme administrateur Fabric.
Ressources de calcul	Sélectionnez les clusters de ressources de calcul que les administrateurs peuvent gérer.

Une fois que vous avez ajouté des ressources de calcul à un groupe Fabric et que vRealize Automation a collecté des données à partir de ceux-ci, les administrateurs Fabric peuvent créer des réservations pour les ressources de calcul.

4 Créez des réservations pour les ressources de calcul de l'instance de vCenter Server.

- a Sélectionnez **Infrastructure > Réservations > Réservations**.
- b Sélectionnez **Nouveau > vSphere (vCenter)**.
- c Dans chaque onglet, entrez les informations pour la réservation.

Option	Action
Général	Sélectionnez une stratégie de réservation, la priorité de la stratégie, puis cliquez sur Activer cette réservation .
Ressources	Sélectionnez le quota de machines, la mémoire et le stockage. Vous n'avez pas besoin de sélectionner un pool de ressources.
Réseau	Sélectionnez l'adaptateur réseau. Vous n'avez pas besoin de sélectionner un profil réseau.
Propriétés	Si nécessaire, ajoutez des propriétés personnalisées à la réservation.
Alerte	Si nécessaire, sélectionnez Alertes de capacité pour notifier les destinataires lorsque la capacité dépasse le seuil de la réservation.

5 Activez la stratégie de positionnement.

- a Sélectionnez **Infrastructure > Réservations > Stratégie de positionnement**.
- b Cochez la case intitulée **Utiliser vRealize Operations Manager pour les recommandations de positionnement**.

Vous avez configuré vRealize Automation pour utiliser l'analyse de vRealize Operations Manager afin de placer les machines lorsque les utilisateurs déploient des blueprints.

Suivant

Configurez vRealize Operations Manager pour surveiller l'instance de vCenter Server et appliquer une stratégie de positionnement de la charge de travail à vos ressources de calcul du cluster. Reportez-vous à [Configurer vRealize Operations Manager pour le positionnement de la charge de travail dans vRealize Automation](#).

Configurer vRealize Operations Manager pour le positionnement de la charge de travail dans vRealize Automation

Pour fournir l'analyse de positionnement de la charge de travail à vRealize Automation afin de placer les machines lorsque vous déployez de nouveaux blueprints, vous devez préparer l'instance de vRealize Operations Manager.

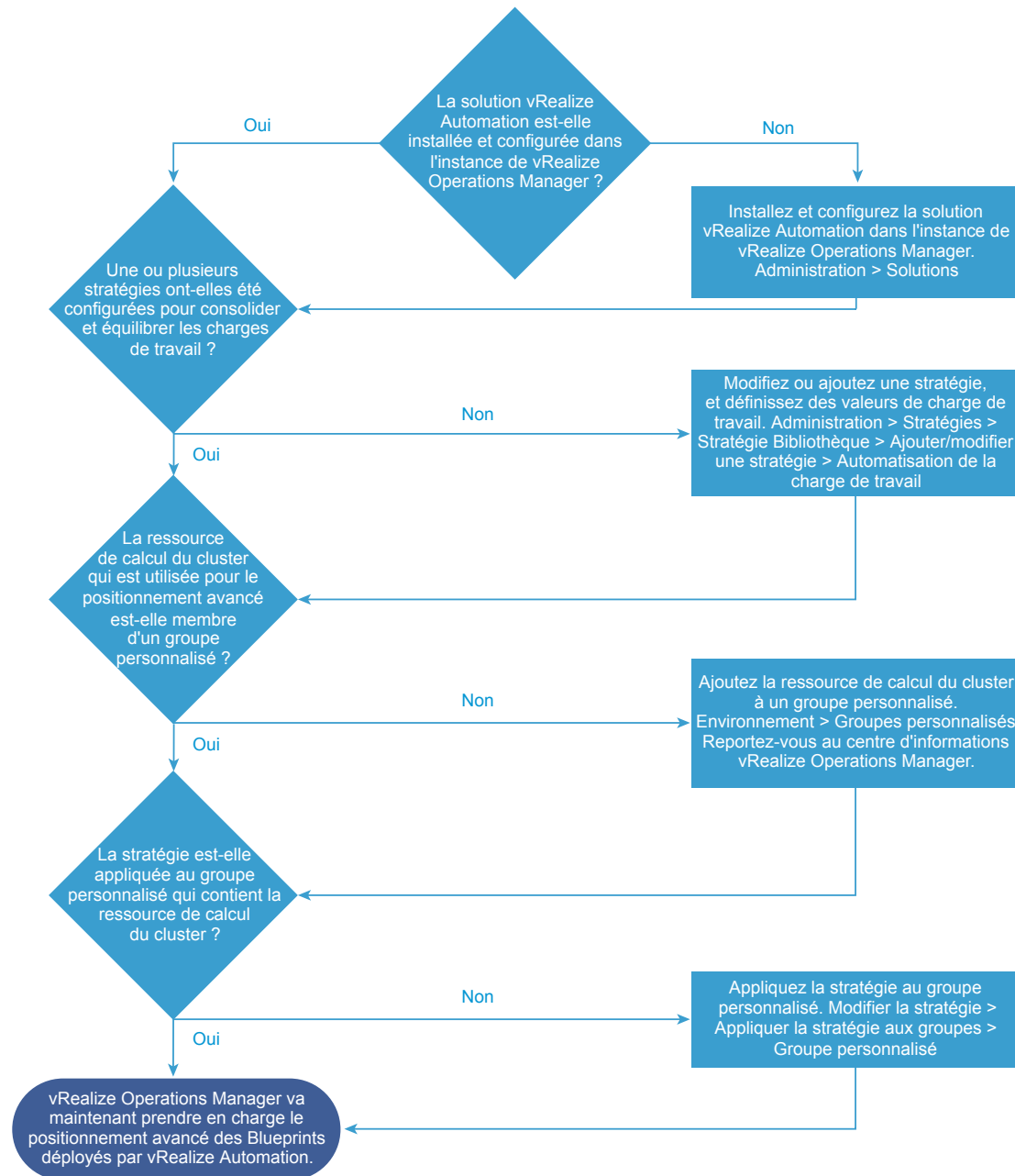
Avertissement Vous ne devez installer la solution vRealize Automation, qui comprend le module de gestion, que sur une seule instance de vRealize Operations Manager.

Pour préparer votre instance de vRealize Operations Manager afin de fournir une analyse à vRealize Automation, vous installez et configurez la solution vRealize Automation. Vous devez également configurer une stratégie et appliquer cette stratégie aux ressources de calcul de votre cluster.

Après avoir configuré la solution vRealize Automation, vous ne pouvez pas déplacer ou rééquilibrer les machines virtuelles que vRealize Automation gère.

Si la solution vRealize Automation n'est pas installée dans l'instance de vRealize Operations Manager, le positionnement de la charge de travail peut toujours déplacer ou rééquilibrer les machines virtuelles que vRealize Automation gère.

Pour permettre au positionnement de la charge de travail de déplacer des machines virtuelles, ces machines virtuelles doivent résider dans un centre de données ou un centre de données personnalisé.



Prérequis

- Configurez vRealize Automation pour utiliser l'analyse de positionnement de la charge de travail. Reportez-vous à [Configurer vRealize Automation pour le positionnement de la charge de travail](#).
- Vérifiez que la solution vRealize Automation est installée et configurée dans l'instance de vRealize Operations Manager qui est utilisée pour le positionnement de la charge de travail. Pour plus d'informations sur cette solution, voir le [module de gestion pour vRealize Automation sur Solution Exchange](#). Pour plus d'informations sur le fonctionnement du positionnement de la charge de travail dans vRealize Operations Manager, reportez-vous à la section [Détails d'automatisation de charge de travail](#) et aux rubriques connexes de la documentation de vRealize Operations Manager.

Procédure

- 1 Dans l'instance de vRealize Operations Manager qui gère le positionnement de la charge de travail, installez et configurez la solution vRealize Automation.

Il est possible que la solution soit déjà installée.

- a Pour voir les solutions qui sont installées dans vRealize Operations Manager, cliquez sur **Administration > Solutions**.

- b Vérifiez si la solution vRealize Automation est déjà installée.

Si la solution vRealize Automation n'apparaît pas dans la liste, téléchargez et installez la solution. Reportez-vous à la section [Module de gestion pour vRealize Automation sur Solution Exchange](#).

- c Si la solution apparaît dans la liste, sélectionnez la **solution VMware vRealize Automation** et cliquez sur **Configurer**.

- d Configurez la solution vRealize Automation et enregistrez les paramètres.

Pour plus d'informations sur la configuration de la solution, reportez-vous à la section [Solutions dans vRealize Operations Manager](#) dans le centre d'informations de vRealize Operations Manager.

- 2 Si vous n'utilisez pas la stratégie par défaut de vRealize Operations Manager, vous devez créer un groupe personnalisé. Ensuite, ajoutez vos ressources de calcul du cluster au groupe personnalisé.

Pour appliquer à vos clusters une stratégie autre que la stratégie par défaut, ajoutez un groupe personnalisé. Vous pouvez ensuite appliquer la stratégie au groupe personnalisé. Si vous utilisez la stratégie par défaut, vous n'avez pas besoin de créer un groupe personnalisé, car la stratégie par défaut s'applique à tous les objets.

- a Cliquez sur **Environnement > Groupes personnalisés**.

- b Si un groupe personnalisé n'existe pas pour vos clusters, créez un groupe personnalisé.

Pour plus d'informations, reportez-vous à la section [Scénario utilisateur : création de groupes d'objets personnalisés](#) dans le centre d'informations de vRealize Operations Manager.

- c Ajoutez le cluster au groupe personnalisé et enregistrez le groupe personnalisé.

- 3 Configurez une stratégie pour consolider et équilibrer les charges de travail sur vos clusters et appliquez cette stratégie au groupe personnalisé.

Vous configurez une stratégie dans vRealize Operations Manager pour définir les paramètres de consolidation, d'équilibrage, de remplissage, de CPU, de mémoire et d'espace disque. Par exemple, vous modifiez le paramètre nommé Consolider les charges de travail afin de déterminer le meilleur positionnement de nouvelles charges de travail gérées en fonction de l'état et de la capacité du cluster. Vous modifiez également le paramétrage de seuil pour équilibrer les charges de travail au niveau d'agressivité requis pour placer les charges de travail. Vous pouvez configurer une ou plusieurs stratégies et les appliquer aux ressources de calcul de vos clusters.

- a Pour localiser les stratégies, cliquez sur **Administration > Stratégies > Bibliothèque de stratégies**.
- b Pour définir des valeurs de charge de travail, cliquez sur **Ajouter/Modifier une stratégie**, puis cliquez sur **Automatisation des charges de travail**.

Les paramètres nommés Consolider les charges de travail et Marge de cluster s'appliquent au positionnement initial des machines virtuelles.

- Lorsque vous définissez Consolider les charges de travail sur **Aucun**, le positionnement de la charge de travail équilibre la charge de travail sur tous les clusters auxquels la stratégie est appliquée. Lorsque vous définissez Consolider les charges de travail sur une valeur autre que Aucun, le positionnement de la charge de travail remplit en priorité le cluster le plus actif.
 - La Marge de cluster est l'espace tampon réservée dans un cluster, en pourcentage de la capacité totale. Par exemple, si vous définissez la marge de cluster à 20 %, ce tampon peut empêcher le positionnement de la charge de travail de placer des machines virtuelles sur ce cluster. La raison pour laquelle il empêche le positionnement est que le cluster a 20 % de capacité en moins que la capacité libre de CPU, de mémoire ou d'espace disque.
- c Dans l'espace de travail des stratégies, cliquez sur **Appliquer la stratégie aux groupes**.
 - d Sélectionnez le groupe personnalisé.
 - e Enregistrez la stratégie.

Vous avez configuré vRealize Operations Manager de sorte que vRealize Automation utilise l'analyse de positionnement de la charge de travail pour suggérer des destinations de positionnement des machines lorsque les utilisateurs déploient des blueprints.

Suivant

Attendez que vRealize Automation et vRealize Operations Manager aient collecté des données depuis les points de terminaison et les objets dans votre environnement. Ensuite, lorsque vous déployez de nouveaux blueprints, vRealize Automation affiche les recommandations de positionnement de la charge de travail, les candidats de destination et le positionnement sélectionné pour votre confirmation.

Dépannage des problèmes de positionnement de la charge de travail

Si vous rencontrez des problèmes avec le positionnement de la charge de travail, utilisez les informations de dépannage pour les résoudre.

La solution vRealize Automation est requise pour que le positionnement de la charge de travail fonctionne correctement

Le positionnement de la charge de travail est basé sur des machines individuelles, et il s'effectue au niveau de la machine. Lorsque vRealize Automation et vRealize Operations Manager sont installés ensemble, la solution vRealize Automation doit également être installée.

La solution, qui inclut le module de gestion et l'adaptateur, identifie les clusters sur lesquels les actions Rééquilibrer le conteneur ou Déplacer la VM sont désactivées. L'action de rééquilibrage est désactivée sur le centre de données personnalisé à laquelle appartient le cluster.

- Pour les clusters vRealize Automation non gérés qui appartiennent à un centre de données personnalisé qui ne dispose pas de clusters vRealize Automation gérés, les actions Déplacer la VM et Rééquilibrer le conteneur sont activées. Pour les clusters vRealize Automation gérés, ces actions sont désactivées.
- Dans vRealize Operations Manager, l'adaptateur vRealize Automation empêche le déplacement ou le rééquilibrage des machines virtuelles sur les clusters qui mappent les réservations.

Avertissement La solution vRealize Automation doit uniquement être installée sur une seule instance de vRealize Operations Manager.

La haute disponibilité (HA) est activée, mais doit être désactivée

Lorsque HA est activée, si vRealize Operations Manager est en panne, le délai d'attente du positionnement de la charge de travail pour appeler vRealize Operations Manager peut échouer

vRealize Automation enregistre les erreurs de placement de la charge de travail dans le fichier journal `catalina.out`.

Les points de terminaison vSphere dans vRealize Automation ne sont pas surveillés

vRealize Operations Manager ne surveille pas l'instance de vCenter Server vSphere contenant les clusters de réservation.

Si vRealize Operations Manager ne reconnaît pas les réservations de candidats vRealize Automation pour un cluster, une banque de données ou un cluster de banque de données quand il tente de les positionner, il les ignore. Dans la réponse de positionnement, vRealize Operations Manager communique à vRealize Automation qu'il ne les reconnaît pas.

Par conséquent, dans les détails du positionnement sur l'exécution de la demande, vRealize Automation affiche une icône d'avertissement sur la réservation de candidats pour indiquer qu'elle n'est pas reconnue.

Lorsque des erreurs de mise en correspondance se produisent, vRealize Automation s'affiche en haut de la liste

vRealize Automation et vRealize Operations Manager gèrent différentes vues de l'infrastructure. Mais ils doivent gérer les mêmes instances de vCenter Server dans une même infrastructure.

Doit identifier les déconnexions et les erreurs de mise en correspondance, et afficher les détails.

Que faire si l'adaptateur vRealize Automation est en panne

Le positionnement initial distingue toujours la liste des destinations possibles qu'il reçoit de vRealize Operations Manager, par exemple lorsqu'un utilisateur ajoute un cluster immédiatement après l'installation.

Si la solution vRealize Automation, qui inclut le module de gestion et l'adaptateur, n'est pas disponible dans vRealize Operations Manager, les actions `déplacer la VM` et `rééquilibrer le conteneur` sont disponibles.

Gestion des paires de clés

Les paires de clés permettent d'effectuer des provisionnements et de se connecter à une instance de cloud. Une paire de clés permet de déchiffrer des mots de passe Windows ou de se connecter à une machine Linux.

Les paires de clés sont nécessaires pour le provisionnement avec Amazon AWS. Pour Red Hat OpenStack, les paires de clés sont facultatives.

Des paires de clés existantes sont importées lors de la collecte de données lorsque vous ajoutez un point de terminaison de cloud. Un administrateur Fabric peut également créer et gérer des paires de clés à l'aide de la console vRealize Automation. Si vous supprimez une paire de clés avec la console vRealize Automation, elle est également supprimée du compte du service de cloud.

Outre la gestion manuelle des paires de clés, vous pouvez configurer vRealize Automation pour générer automatiquement des paires de clés par machine ou par groupe d'activité.

- Un administrateur Fabric peut configurer la génération automatique de paires de clés au niveau d'une réservation.
- Si la paire de clés doit être contrôlée au niveau du Blueprint, l'administrateur Fabric doit sélectionner **Non spécifiée** dans la réservation.
- Un administrateur de locataire ou un gestionnaire de groupes d'activité peut configurer la génération automatique de paires de clés au niveau d'un Blueprint.
- Si la génération de paires de clés configurée au niveau de la réservation et du Blueprint, le paramètre de la réservation remplace celui du Blueprint.

Créer une paire de clés

Vous pouvez créer des paires de clés à utiliser avec les points de terminaison à l'aide de vRealize Automation.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur Fabric**.
- Créez un point de terminaison et ajoutez vos ressources de calcul cloud à un groupe Fabric. Reportez-vous à la section [Choisir un scénario de point de terminaison](#) et [Créer un groupe Fabric](#).

Procédure

- 1 Sélectionnez **Infrastructure > Réservations > Paires de clés**.
- 2 Cliquez sur **Nouveau**.
- 3 Entrez un nom dans la zone de texte **Nom**.
- 4 Sélectionnez une région de cloud dans le menu déroulant **Ressource de calcul**.
- 5 Cliquez sur l'icône **Enregistrer** (✓).

La paire de clés est prête à être utilisée lorsque la colonne Clé secrète contient la valeur *****.

Télécharger la clé privée pour une paire de clés

Vous pouvez télécharger la clé privée pour une paire de clés au format PEM.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur Fabric**.
- Vous devez déjà disposer d'une paire de clés. Reportez-vous à [Créer une paire de clés](#).

Procédure

- 1 Sélectionnez **Infrastructure > Réservations > Paires de clés**.
- 2 Recherchez la paire de clés pour laquelle vous souhaitez télécharger une clé privée.
- 3 Cliquez sur l'icône **Modifier** (✎).
- 4 Utilisez l'une des méthodes suivantes pour télécharger la clé.
 - Recherchez un fichier codé au format PEM et cliquez sur **Télécharger**.
 - Collez le texte de la clé privée commençant par -----BEGIN RSA PRIVATE KEY----- et finissant par -----END RSA PRIVATE KEY-----.
- 5 Cliquez sur l'icône **Enregistrer** (✓).

Exporter la clé privée d'une paire de clés

Vous pouvez exporter la clé privée d'une paire de clés dans un fichier encodé dans le format PEM.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur Fabric**.
- Une paire de clés avec une clé privée doit exister. Reportez-vous à [Télécharger la clé privée pour une paire de clés](#).

Procédure

- 1 Sélectionnez **Infrastructure > Réservations > Paires de clés**.
- 2 Localisez la paire de clés à partir de laquelle exporter la clé privée.
- 3 Cliquez sur l'icône **Exporter** (📄).
- 4 Accédez à l'emplacement dans lequel vous souhaitez enregistrer le fichier et cliquez sur **Enregistrer**.

Scénario : appliquer un emplacement à une ressource de calcul pour des déploiements inter-région

En tant qu'administrateur Fabric, vous souhaitez étiqueter vos ressources de calcul comme appartenant au centre de données de Boston ou de Londres, afin de prendre en charge les déploiements inter-région. Lorsque les architectes de Blueprint activent la fonctionnalité des emplacements sur leurs Blueprints, les utilisateurs peuvent choisir de provisionner des machines du centre de données de Boston ou de Londres.



Vous voulez éviter que les utilisateurs du centre de données de Boston ne provisionnent des machines de l'infrastructure de Londres, et que les utilisateurs du centre de données de Londres ne provisionnent des machines de l'infrastructure de Boston. Pour vous assurer que les utilisateurs de Boston ne provisionnent que l'infrastructure de Boston, et ceux de Londres celle de Londres uniquement, vous souhaitez autoriser les utilisateurs à sélectionner l'emplacement de provisionnement adéquat lors de leur demande de machines.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur Fabric**.
- En tant qu'administrateur système, définissez les emplacements de centre de données. Reportez-vous à [Scénario : ajouter des emplacements de centre de données pour des déploiements inter-région](#).

Procédure

- 1 Sélectionnez **Infrastructure > Ressources de calcul > Ressources de calcul**.
- 2 Pointez vers une ressource de calcul du centre de données de Boston et cliquez sur **Modifier**.
- 3 Dans le menu déroulant **Emplacements**, sélectionnez Boston.
- 4 Cliquez sur **OK**.

- 5 Si nécessaire, répétez cette procédure pour associer les ressources de calcul aux emplacements de Boston et de Londres.

Les architectes IaaS peuvent activer la fonctionnalité des emplacements afin que les utilisateurs puissent choisir de provisionner des machines de Boston ou de Londres lorsqu'ils complètent leurs formulaires de demande d'éléments du catalogue. Reportez-vous à [Scénario : permettre aux utilisateurs de sélectionner des emplacements de centre de données pour des déploiements inter-région](#).

Provisionnement d'un déploiement vRealize Automation à l'aide d'un fournisseur IPAM tiers

Vous pouvez obtenir des adresses IP et des plages à utiliser dans un profil réseau vRealize Automation d'un fournisseur de solutions IPAM tiers pris en charge, tel qu'Infoblox.

Les plages d'adresses IP du profil réseau sont utilisées dans une réservation associée que vous spécifiez dans un Blueprint. Lorsqu'un utilisateur autorisé demande un provisionnement de machine en utilisant l'élément de catalogue du Blueprint, une adresse IP est obtenue à partir de la plage d'adresses IP spécifiée par le fournisseur IPAM tiers. Après le déploiement de la machine, vous pouvez découvrir l'adresse IP utilisée en interrogeant sa page de détails d'éléments vRealize Automation.

Tableau 2-19. Préparation du provisionnement d'un déploiement vRealize Automation en utilisant la liste de contrôle Infoblox IPAM

Tâche	Description	Détails
Obtenez, importez et configurez le plug-in ou le module du fournisseur de solutions IPAM tiers.	Obtenez et importez le plug-in vRealize Orchestrator, exécutez les workflows de configuration de vRealize Orchestrator et enregistrez le type de point de terminaison de fournisseur IPAM dans vRealize Orchestrator. Si VMware Solution Exchange à l'adresse https://marketplace.vmware.com/vsx ne contient pas le module du fournisseur IPAM dont vous avez besoin, vous pouvez créer votre propre module en utilisant le kit de développement logiciel du fournisseur de solutions IPAM et la documentation connexe. Consultez la page vRealize Automation Third-Party IPAM Integration SDK 7.3 à l'adresse code.vmware.com .	Reportez-vous à Liste de contrôle pour assurer la prise en charge d'un fournisseur IPAM tiers .
Créez un point de terminaison de fournisseur de solutions IPAM tiers.	Créez un nouveau point de terminaison IPAM dans vRealize Automation.	Reportez-vous à Créer un point de terminaison de fournisseur IPAM tiers .
Spécifiez les paramètres de point de terminaison du fournisseur de solutions IPAM tiers dans un profil réseau externe.	Créez un profil réseau externe et spécifiez le point de terminaison IPAM dans vRealize Automation.	Reportez-vous à Créer un profil de réseau externe au moyen d'un fournisseur IPAM tiers .
Spécifiez éventuellement les paramètres de point de terminaison du fournisseur de solutions IPAM tiers dans un profil réseau acheminé	Créez un profil réseau à la demande et spécifiez le point de terminaison IPAM défini dans vRealize Automation.	Reportez-vous à Créer un profil de réseau acheminé au moyen d'un point de terminaison IPAM tiers ou Créer un profil de réseau NAT au moyen d'un point de terminaison IPAM tiers .

Tableau 2-19. Préparation du provisionnement d'un déploiement vRealize Automation en utilisant la liste de contrôle Infoblox IPAM (suite)

Tâche	Description	Détails
Définissez une réservation afin d'utiliser le profil réseau.	Créez une réservation qui appelle le profil réseau dans vRealize Automation.	Reportez-vous à Créer une réservation pour Hyper-V, KVM, SCVMM, vSphere ou XenServer .
Définissez un Blueprint qui utilise le profil réseau externe.	Créez un Blueprint qui utilise la réservation dans vRealize Automation.	Reportez-vous à Chapitre 3 Fourniture de Blueprints de service aux utilisateurs .
Publiez le Blueprint dans le catalogue pour le rendre accessible et utilisable.	Publiez le Blueprint au catalogue dans vRealize Automation. Ajoutez les droits d'accès requis.	Reportez-vous à Publier un Blueprint .
Demandez le provisionnement de machine en utilisant l'élément du catalogue de Blueprints.	Utilisez l'élément de catalogue du Blueprint pour demander le provisionnement de machine dans vRealize Automation.	Reportez-vous à Gestion du catalogue de services .

Configuration des ressources XaaS

En configurant les points de terminaison XaaS, vous pouvez connecter l'instance de vRealize Automation à votre environnement. Lorsque vous configurez des plug-ins vRealize Orchestrator comme points de terminaison, utilisez l'interface utilisateur vRealize Automation au lieu de l'interface de configuration vRealize Orchestrator.

Pour utiliser les capacités vRealize Orchestrator et les plug-ins vRealize Orchestrator afin d'exposer les technologies VMware et les technologies tierces à vRealize Automation, vous pouvez configurer les plug-ins vRealize Orchestrator en les ajoutant comme points de terminaison. Ainsi, vous créez des connexions vers différents hôtes et serveurs, tels que des instances de vCenter Server ou un hôte Microsoft Active Directory.

Lorsque vous ajoutez un plug-in vRealize Orchestrator comme point de terminaison à l'aide de l'interface utilisateur vRealize Automation, exécutez un workflow de configuration dans le serveur vRealize Orchestrator par défaut. Les workflows de configuration résident dans le dossier de workflows **vRealize Automation > XaaS > Configuration du point de terminaison**.

Important La configuration d'un plug-in unique dans vRealize Orchestrator et dans la console vRealize Automation n'est pas prise en charge et produit des erreurs.

Configurer le plug-in Active Directory comme un point de terminaison

Vous ajoutez un point de terminaison et configurez le plug-in Active Directory afin de le connecter à une instance d'Active Directory en cours d'exécution. Vous pouvez ainsi gérer notamment les utilisateurs et les groupes d'utilisateurs, les ordinateurs Active Directory et les unités d'organisation.

Après avoir ajouté un point de terminaison Active Directory, vous pouvez le mettre à jour à tout moment.

Prérequis

- Vérifiez que vous avez accès à une instance de Microsoft Active Directory. Reportez-vous à la documentation relative à Microsoft Active Directory.
- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

- 1 Sélectionnez **Administration > Points de terminaison > Points de terminaison Orchestrator**.
- 2 Cliquez sur l'icône **Nouveau** (+).
- 3 Dans le menu déroulant **Plug-in**, sélectionnez **Active Directory**.
- 4 Cliquez sur **Suivant**.
- 5 Entrez un nom et, éventuellement, une description.
- 6 Cliquez sur **Suivant**.
- 7 Configurez les détails du serveur Active Directory.
 - a Dans la zone de texte **IP/URL de l'hôte Active Directory**, entrez l'adresse IP ou le nom DNS de l'hôte sur lequel Active Directory est exécuté.
 - b Dans la zone de texte **Port**, entrez le port de recherche du serveur Active Directory.

vRealize Orchestrator prend en charge la structure de domaines hiérarchique Active Directory. Si le contrôleur de domaine est configuré pour utiliser le catalogue global, utilisez le port 3268. Vous ne pouvez pas utiliser le port par défaut 389 pour vous connecter au serveur du catalogue global. Outre les ports 389 et 3268, vous pouvez utiliser 636 pour LDAPS.
 - c Dans la zone de texte **Racine**, entrez l'élément racine du service Active Directory.

Par exemple, si votre nom de domaine est *mycompany.com*, l'élément racine du service Active Directory racine est **dc=mycompany,dc=com**.

Ce nœud sert à parcourir le répertoire de services après avoir entré les informations d'identification appropriées. Si le répertoire de services est volumineux, spécifiez un nœud de l'arborescence afin de limiter la recherche et d'améliorer les performances. Par exemple, plutôt que d'exécuter une recherche dans l'intégralité du répertoire, spécifiez **ou=employees,dc=mycompany,dc=com**. Cet élément racine affiche tous les utilisateurs qui appartiennent au groupe Employés.
 - d (Facultatif) Pour activer la certification chiffrée de la connexion entre vRealize Orchestrator et Active Directory, sélectionnez **Oui** dans le menu déroulant **Utiliser SSL**.

L'importation du certificat SSL est automatique et ne déclenche aucune invite de confirmation, même s'il est autosigné.
 - e (Facultatif) Entrez le domaine dans la zone de texte **Domaine par défaut**.

Par exemple, si votre nom de domaine est *mycompany.com*, tapez **@mycompany.com**.

8 Configurez les paramètres de la session partagée.

Les informations d'identification sont utilisées par vRealize Orchestrator pour exécuter tous les workflows et actions Active Directory.

- a Dans la zone de texte **Nom d'utilisateur de la session partagée**, entrez le nom d'utilisateur correspondant.
- a Dans la zone de texte **Mot de passe de la session partagée**, entrez le mot de passe correspondant.

9 Cliquez sur **Terminer**.

Vous avez désormais ajouté une instance d'Active Directory en tant que point de terminaison. Les architectes XaaS peuvent utiliser XaaS afin de publier des workflows du plug-in Active Directory en tant qu'éléments du catalogue et actions sur la ressource.

Suivant

- Pour utiliser des Blueprints vRealize Automation pour gérer vos utilisateurs Active Directory dans votre environnement, créez un Blueprint XaaS basé sur Active Directory. Par exemple, reportez-vous à [Créer un Blueprint XaaS ainsi qu'une action visant à créer et à modifier un utilisateur](#).
- Pour utiliser vRealize Automation pour créer des enregistrements Active Directory lorsqu'une machine est déployée, vous pouvez créer différentes stratégies Active Directory et les appliquer à différents groupes d'activité et Blueprints. Reportez-vous à [Créer et appliquer des stratégies Active Directory](#).

Configurer le plug-in HTTP-REST comme un point de terminaison

Vous pouvez ajouter un point de terminaison et configurer le plug-in HTTP-REST pour vous connecter à un hôte REST.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.
- Vérifiez que vous avez accès à un hôte REST.

Procédure

- 1 Sélectionnez **Administration > Points de terminaison > Points de terminaison Orchestrator**.
- 2 Cliquez sur l'icône **Nouveau (+)**.
- 3 Sélectionnez **HTTP-REST** dans le menu déroulant **Plug-in**.
- 4 Cliquez sur **Suivant**.
- 5 Entrez un nom et, éventuellement, une description.
- 6 Cliquez sur **Suivant**.

7 Renseignez les informations concernant l'hôte REST.

- a Dans la zone de texte **Nom**, entrez le nom de l'hôte.
- b Entrez l'adresse de l'hôte dans la zone de texte **URL**.

Remarque Si vous utilisez l'authentification d'accès Kerberos, vous devez fournir l'adresse de l'hôte sous la forme d'un nom de domaine complet.

- c (Facultatif) Entrez le nombre de secondes avant l'expiration d'une connexion dans la zone de texte **Délai d'expiration de connexion (secondes)**.

La valeur par défaut est 30 secondes.

- d (Facultatif) Entrez le nombre de secondes avant l'expiration d'une opération dans la zone de texte **Délai d'expiration de l'opération (secondes)**.

La valeur par défaut est 60 secondes.

8 (Facultatif) Configurez les paramètres de proxy.

- a Pour utiliser un proxy, sélectionnez **Oui** dans le menu déroulant **Utiliser le proxy**.
- b Entrez l'adresse IP du serveur de proxy dans la zone de texte **Adresse du proxy**.
- c Entrez le numéro du port pour communiquer avec le serveur proxy dans la zone de texte **Port du proxy**.

9 Cliquez sur **Suivant**.

10 Sélectionnez le type d'authentification.

Option	Action
Aucun	Aucune authentification n'est requise.
OAuth 1.0	<p>Utilise le protocole OAuth 1.0. Vous devez indiquer les paramètres d'authentification requis sous OAuth 1.0.</p> <ul style="list-style-type: none"> a Entrez la clé utilisée pour identifier le consommateur comme un fournisseur de service dans la zone de texte Clé consommateur. b Entrez le code secret permettant d'établir la propriété de la clé consommateur dans la zone de texte Code secret consommateur. c (Facultatif) Entrez le jeton d'accès que le consommateur utilise pour accéder aux ressources protégées dans la zone de texte Jeton d'accès. d (Facultatif) Entrez le code secret que le consommateur utilise pour établir la propriété d'un jeton dans la zone de texte Code secret de jeton d'accès.
OAuth 2.0	<p>Utilise le protocole OAuth 2.0.</p> <p>Entrez le jeton d'authentification dans la zone de texte Jeton.</p>
De base	<p>Fournit une authentification de l'accès de base. La communication avec l'hôte est en mode de session partagée.</p> <ul style="list-style-type: none"> a Entrez le nom d'utilisateur pour la session partagée dans la zone de texte Nom d'utilisateur d'authentification. b Entrez le mot de passe pour la session partagée dans la zone de texte Nom d'utilisateur d'authentification.

Option	Action
Prétraitement	<p>Fournit une authentification d'accès de prétraitement qui utilise le chiffrement. La communication avec l'hôte est en mode de session partagée.</p> <ol style="list-style-type: none"> Entrez le nom d'utilisateur pour la session partagée dans la zone de texte Nom d'utilisateur d'authentification. Entrez le mot de passe pour la session partagée dans la zone de texte Nom d'utilisateur d'authentification.
NTLM	<p>Fournit une authentification d'accès NT LAN Manager (NTLM) au sein de la structure Window Security Support Provider (SSP). La communication avec l'hôte est en mode de session partagée.</p> <ol style="list-style-type: none"> Renseignez les informations d'identification pour la session partagée. <ul style="list-style-type: none"> Entrez le nom d'utilisateur pour la session partagée dans la zone de texte Nom d'utilisateur d'authentification. Entrez le mot de passe pour la session partagée dans la zone de texte Nom d'utilisateur d'authentification. Configurez les détails NTLM. <ul style="list-style-type: none"> (Facultatif) Entrez le nom de la station de travail dans la zone de texte Station de travail pour authentification NTLM. Entrez le nom de domaine dans la zone de texte Domaine pour authentification NTLM.
Kerberos	<p>Fournit une authentification de l'accès Kerberos. La communication avec l'hôte est en mode de session partagée.</p> <ol style="list-style-type: none"> Entrez le nom d'utilisateur pour la session partagée dans la zone de texte Nom d'utilisateur d'authentification. Entrez le mot de passe pour la session partagée dans la zone de texte Nom d'utilisateur d'authentification.

11 Cliquez sur **Terminer**.

Vous avez configuré le point de terminaison et ajouté un hôte REST. Les architectes XaaS peuvent utiliser XaaS pour publier des workflows de plug-in HTTP-REST en tant qu'éléments du catalogue et actions sur les ressources.

Configurer le plug-in PowerShell en tant que point de terminaison

Vous pouvez ajouter un point de terminaison et configurer le plug-in PowerShell afin de le connecter à un hôte PowerShell en cours d'exécution. Ainsi, vous pouvez appeler des scripts et des applets de commande PowerShell à partir d'actions et de workflows vRealize Orchestrator, puis utiliser le résultat obtenu selon vos besoins.

Prérequis

- Vérifiez que vous disposez d'un accès à un hôte Windows PowerShell. Pour plus d'informations sur Microsoft Windows PowerShell, consultez la documentation relative à Windows PowerShell.
- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

- 1 Sélectionnez **Administration > Points de terminaison > Points de terminaison Orchestrator**.

- 2 Cliquez sur l'icône **Nouveau** (+).
- 3 Dans le menu déroulant **Plug-in**, sélectionnez **PowerShell**.
- 4 Cliquez sur **Suivant**.
- 5 Entrez un nom et, éventuellement, une description.
- 6 Cliquez sur **Suivant**.
- 7 Spécifiez les détails de l'hôte PowerShell.
 - a Dans la zone de texte **Nom**, entrez le nom de l'hôte.
 - b Dans la zone de texte **Hôte/IP**, entrez l'adresse IP ou le nom de domaine complet de l'hôte (FDQN, Full Domain Qualified Name).
- 8 Sélectionnez le type d'hôte PowerShell auquel le plug-in doit se connecter.

Option	Action
WinRM	<ol style="list-style-type: none"> a Dans la zone de texte Port sous les détails de l'hôte PowerShell, entrez le numéro de port à utiliser pour communiquer avec l'hôte. b Dans le menu déroulant Protocole de transport, sélectionnez le protocole de votre choix. <p>Remarque Si vous utilisez le protocole de transport HTTPS, le certificat de l'hôte PowerShell distant est importé dans le keystore vRealize Orchestrator.</p> <ol style="list-style-type: none"> c Dans le menu déroulant Authentification, sélectionnez le type d'authentification. <p>Remarque Pour utiliser l'authentification Kerberos, activez-la dans le service WinRM. Pour plus d'informations sur la configuration de l'authentification Kerberos, reportez-vous à <i>Utilisation du plug-in PowerShell</i>.</p>
SSH	Aucune.

- 9 Dans les zones de texte **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification d'une communication en session partagée avec l'hôte PowerShell.
- 10 Cliquez sur **Terminer**.

Vous avez ajouté un hôte PowerShell en tant que point de terminaison. Les architectes XaaS peuvent utiliser l'instance de XaaS afin de publier des workflows du plug-in PowerShell en tant qu'éléments du catalogue et actions sur la ressource.

Configurer le plug-in SOAP comme un point de terminaison

Vous pouvez ajouter un point de terminaison et configurer le plug-in SOAP afin de définir un service SOAP en tant qu'objet d'inventaire, et réaliser des opérations SOAP sur les objets définis.

Prérequis

- Vérifiez que vous avez accès à un hôte SOAP. Le plug-in prend en charge les versions de SOAP 1.1 et 1.2, et les versions de WSDL 1.1 et 2.0.
- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

- 1 Sélectionnez **Administration > Points de terminaison > Points de terminaison Orchestrator**.
- 2 Cliquez sur l'icône **Nouveau** (+).
- 3 Dans le menu déroulant **Plug-in**, sélectionnez **SOAP**.
- 4 Cliquez sur **Suivant**.
- 5 Entrez un nom et, éventuellement, une description.
- 6 Cliquez sur **Suivant**.
- 7 Fournissez les détails de l'hôte SOAP.
 - a Dans la zone de texte **Nom**, entrez le nom de l'hôte.
 - b Dans le menu déroulant **Fournir un contenu WSDL**, déterminez si le contenu WSDL doit être fourni sous forme de texte.

Option	Action
Oui	Dans la zone de texte Contenu WSDL , entrez le texte WSDL.
Non	Dans la zone de texte URL WSDL , entrez le chemin d'accès.
 - c (Facultatif) Dans la zone de texte **Expiration du délai de connexion (en secondes)**, entrez le nombre de secondes qui doit s'écouler avant l'expiration du délai de connexion.
La valeur par défaut est 30 secondes.
 - d (Facultatif) Dans la zone de texte **Expiration du délai de requête (en secondes)**, entrez le nombre de secondes qui doit s'écouler avant l'expiration d'une opération.
La valeur par défaut est 60 secondes.
- 8 (Facultatif) Spécifiez les paramètres de proxy.
 - a Pour utiliser un proxy, sélectionnez **Oui** dans le menu déroulant **Proxy**.
 - b Dans la zone de texte **Adresse**, entrez l'adresse IP du serveur proxy.
 - c Dans la zone de texte **Port**, entrez le numéro de port permettant de communiquer avec le serveur proxy.
- 9 Cliquez sur **Suivant**.
- 10 Sélectionnez le type d'authentification.

Option	Action
Aucun	Aucune authentification n'est requise.
De base	Fournit une authentification de l'accès de base. La communication avec l'hôte est en mode de session partagée. <ol style="list-style-type: none"> a Dans la zone de texte Nom d'utilisateur, entrez le nom d'utilisateur de la session partagée. b Dans la zone de texte Mot de passe, entrez le mot de passe de la session partagée.

Option	Action
Prétraitement	<p>Fournit une authentification d'accès de prétraitement qui utilise le chiffrement. La communication avec l'hôte est en mode de session partagée.</p> <ol style="list-style-type: none"> Dans la zone de texte Nom d'utilisateur, entrez le nom d'utilisateur de la session partagée. Dans la zone de texte Mot de passe, entrez le mot de passe de la session partagée.
NTLM	<p>Fournit une authentification de l'accès NT LAN Manager (NTLM) dans l'infrastructure Security Support Provider (SSP) de Windows. La communication avec l'hôte est en mode de session partagée.</p> <ol style="list-style-type: none"> Fournit les informations d'identification de l'utilisateur. <ul style="list-style-type: none"> Dans la zone de texte Nom d'utilisateur, entrez le nom d'utilisateur de la session partagée. Dans la zone de texte Mot de passe, entrez le mot de passe de la session partagée. Fournit les paramètres NTLM. <ul style="list-style-type: none"> Dans la zone de texte Domaine NTLM, entrez le nom de domaine. (Facultatif) Dans la zone de texte Poste de travail NTLM, entrez le nom du poste de travail.
Négociateur	<p>Fournit une authentification de l'accès Kerberos. La communication avec l'hôte est en mode de session partagée.</p> <ol style="list-style-type: none"> Fournit les informations d'identification de l'utilisateur. <ol style="list-style-type: none"> Dans la zone de texte Nom d'utilisateur, entrez le nom d'utilisateur de la session partagée. Dans la zone de texte Mot de passe, entrez le mot de passe de la session partagée. Dans la zone de texte SPN du service Kerberos, entrez le nom du service principal (SPN, Service Principal Name).

11 Cliquez sur **Terminer**.

Vous avez ajouté un service SOAP. Les architectes XaaS peuvent utiliser XaaS afin de publier des workflows du plug-in SOAP en tant qu'éléments du catalogue et actions sur la ressource.

Configurer le plug-in vCenter Server en tant que point de terminaison

Vous pouvez ajouter un point de terminaison et configurer le plug-in vCenter Server afin d'établir une connexion à une instance de vCenter Server en cours de fonctionnement et créer des Blueprints XaaS pour gérer des objets d'inventaire vSphere.

Prérequis

- Installez et configurez vCenter Server. Reportez-vous à *Installation et configuration de vSphere*.
- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

- 1 Sélectionnez **Administration > Points de terminaison > Points de terminaison Orchestrator**.
- 2 Cliquez sur l'icône **Nouveau** (+).

- 3 Dans le menu déroulant **Plug-in**, sélectionnez **vCenter Server**.
- 4 Cliquez sur **Suivant**.
- 5 Entrez un nom et, éventuellement, une description.
- 6 Cliquez sur **Suivant**.
- 7 Fournissez les informations relatives à l'instance de vCenter Server.
 - a Dans la zone de texte **IP ou nom d'hôte de l'instance de vCenter Server à ajouter**, entrez l'adresse IP ou le nom DNS de la machine.

Il s'agit de l'adresse IP ou du nom DNS de la machine sur laquelle l'instance de vCenter Server à ajouter est installée.
 - b Dans la zone de texte **Port de l'instance de vCenter Server**, entrez le port qui permet de communiquer avec l'instance de vCenter Server.

Le port par défaut est 443.
 - c Dans la zone de texte **Emplacement de l'instance de SDK à utiliser pour la connexion à l'instance de vCenter Server**, entrez l'emplacement correspondant pour la connexion à l'instance de vCenter Server.

Par exemple, `/sdk`.
- 8 Cliquez sur **Suivant**.
- 9 Définissez les paramètres de connexion.
 - a Dans la zone de texte **Port HTTP de l'instance de vCenter Server (applicable au plug-in VC 5.5.2 ou une version précédente)**, entrez le port HTTP de l'instance de vCenter Server.
 - b Dans les zones de texte **Nom d'utilisateur dont Orchestrator se servira pour se connecter à l'instance de vCenter Server**, et **Mot de passe de l'utilisateur dont Orchestrator se servira pour se connecter à l'instance de vCenter Server**, entrez les informations d'identification de vRealize Orchestrator nécessaires à l'établissement de la connexion à l'instance de vCenter Server.

L'utilisateur que vous sélectionnez doit être un utilisateur valide et qui dispose de privilèges permettant de gérer les extensions vCenter Server ainsi qu'un ensemble de privilèges personnalisés.
- 10 Cliquez sur **Terminer**.

Vous avez ajouté une instance de vCenter Server en tant que point de terminaison. Les architectes XaaS peuvent utiliser l'instance de XaaS afin de publier des workflows du plug-in vCenter Server en tant qu'éléments du catalogue et actions sur la ressource.

Créer un point de terminaison Microsoft Azure

Vous pouvez créer un point de terminaison Microsoft Azure pour faciliter une connexion avec informations d'identification entre vRealize Automation et un déploiement Azure.

Un point de terminaison établit une connexion à une ressource, dans ce cas une instance d'Azure, que vous pouvez utiliser pour créer des Blueprints de machine virtuelle. Vous devez disposer d'un point de terminaison Azure comme base des Blueprints pour le provisionnement de machines virtuelles Azure. Si vous utilisez plusieurs abonnements Azure, des points de terminaison seront nécessaires pour chaque ID d'abonnement.

Vous pouvez également créer une connexion Azure directement à partir de vRealize Orchestrator en utilisant la commande d'ajout d'une connexion Azure située sous **Bibliothèque > Azure > Configuration** dans l'arborescence du workflow vRealize Orchestrator. Dans la plupart des cas, il est recommandé de créer une connexion en configurant des points de terminaison comme décrit dans le présent document.

Les points de terminaison Azure sont pris en charge par vRealize Orchestrator et par la fonctionnalité XaaS. Vous pouvez créer, supprimer ou modifier un point de terminaison Azure. Notez que si vous apportez des modifications à un point de terminaison existant et n'exécutez pas de mises à jour sur le portail Azure via la connexion mise à jour pendant plusieurs heures, vous devez redémarrer le service vRealize Orchestrator à l'aide de la commande `service vco-service restart`. Le fait de ne pas redémarrer le service risque de provoquer des erreurs.

Prérequis

- Configurez une instance de Microsoft Azure et obtenez un abonnement valide à Microsoft Azure à partir duquel vous pouvez utiliser l'ID d'abonnement. Reportez-vous à <http://www.vaficionado.com/2016/11/using-new-microsoft-azure-endpoint-vrealize-automation-7-2/> pour plus d'informations sur la configuration d'Azure et l'obtention d'un ID d'abonnement.
- Votre déploiement vRealize Automation doit comporter au moins un locataire et un groupe d'activité.
- Créez une application Active Directory comme indiqué dans <https://azure.microsoft.com/fr-fr/documentation/articles/resource-group-create-service-principal-portal>.
- Prenez note des informations suivantes concernant Azure. Vous en aurez besoin lors de la configuration des points de terminaison et des Blueprints.
 - ID de l'abonnement
 - ID du locataire
 - nom du compte de stockage
 - nom du groupe de ressources
 - emplacement
 - nom du réseau virtuel
 - ID de l'application cliente
 - clé secrète de l'application cliente
 - image de machine virtuelle URN
- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

- 1 Sélectionnez **Administration > Points de terminaison > Points de terminaison Orchestrator**.
- 2 Cliquez sur l'icône **Nouveau (+)**.
- 3 Dans l'onglet Plug-in, cliquez sur le menu déroulant **Plug-in** et sélectionnez Plug-in Azure.
- 4 Cliquez sur **Suivant**.
- 5 Entrez un nom et, éventuellement, une description.
- 6 Cliquez sur **Suivant**.
- 7 Renseignez les zones de texte dans l'onglet **Détails** en fonction du point de terminaison.

Paramètre	Description
Paramètres de connexion	
Connexion Azure	
Nom de la connexion	Nom unique de la connexion du nouveau point de terminaison. Ce nom figure dans l'interface de vRealize Orchestrator pour vous aider à identifier une connexion particulière.
ID d'abonnement Azure	Identifiant de votre abonnement Azure. L'ID définit les comptes de stockage, les machines virtuelles et autres ressources Azure auxquelles vous avez accès.
Paramètres du Gestionnaire de ressources	
URI du service Azure	L'URI par lequel vous pouvez accéder à votre instance d'Azure. La valeur par défaut <code>https://management.azure.com/</code> convient à de nombreuses implémentations type.
ID de locataire	ID du locataire Azure que vous souhaitez que le point de terminaison utilise.
ID client	ID du client Azure que vous souhaitez que le point de terminaison utilise. Ceci est affecté lorsque vous créez une application Active Directory.
Clé secrète client	La clé utilisée avec un ID client Azure. Cette clé est affectée lorsque vous créez une application Active Directory.
URL de connexion	URL utilisée pour accéder à l'instance d'Azure. La valeur par défaut <code>https://login.windows.net/</code> convient à de nombreuses implémentations type.
Paramètres du proxy	
Hôte proxy	Si votre organisation utilise un serveur proxy Web, entrez le nom d'hôte de ce serveur.
Port du proxy	Si votre organisation utilise un serveur proxy Web, entrez le numéro de port de ce serveur.

- 8 Cliquez sur **Terminer**.

Suivant

Créez des groupes de ressources, des comptes de stockage et des groupes de sécurité réseau Azure appropriés. Vous devez également créer des équilibres de charge si approprié pour votre implémentation.

Action	Options
Créer un groupe de ressources Azure	<ul style="list-style-type: none"> ■ Créez le groupe de ressources à l'aide du portail Azure. Reportez-vous à la documentation d'Azure pour obtenir des instructions spécifiques. ■ Utilisez le workflow vRealize Orchestrator approprié se trouvant sous le groupe de ressources <code>Library/Azure/Resource/Create</code>. ■ Dans vRealize Automation, créez et publiez un Blueprint XaaS contenant le workflow vRealize Orchestrator. Vous pouvez demander le groupe de ressources après son attachement au service et aux droits. Notez que le type de ressource du groupe de ressources n'est pas pris en charge ou géré par vRealize Automation.
Créer un compte de stockage Azure	<ul style="list-style-type: none"> ■ Utilisez Azure pour créer un compte de stockage. Reportez-vous à la documentation d'Azure pour obtenir des instructions spécifiques. ■ Utilisez le workflow vRealize Orchestrator approprié se trouvant sous le compte de stockage <code>Library/Azure/Storage/Create storage account</code>. ■ Dans vRealize Automation, créez et publiez un Blueprint XaaS contenant le workflow vRealize Orchestrator. Vous pouvez demander le compte de stockage après son attachement au service et aux droits.
Créer un groupe de sécurité réseau Azure	<ul style="list-style-type: none"> ■ Utilisez Azure pour créer un groupe de sécurité. Reportez-vous à la documentation d'Azure pour obtenir des instructions spécifiques. ■ Utilisez le workflow vRealize Orchestrator approprié se trouvant dans le groupe de sécurité <code>Library/Azure/Network/Create</code>. ■ Dans vRealize Automation, créez et publiez un Blueprint XaaS contenant le workflow vRealize Orchestrator. Vous pouvez demander le groupe de sécurité après son attachement au service et aux droits.

Création et configuration de conteneurs

Vous pouvez utiliser l'onglet Conteneurs dans vRealize Automation pour ouvrir l'application intégrée Conteneurs pour vRealize Automation et créer et configurer les conteneurs et leurs paramètres réseau afin de les rendre disponibles pour les architectes Blueprint vRealize Automation.

Vous pouvez définir des conteneurs en utilisant de nouvelles images et de nouveaux modèles ou ceux qui existent déjà dans l'application intégrée Conteneurs. Vous pouvez ensuite ajouter aux Blueprints vRealize Automation les composants des conteneurs et leurs paramètres réseau associés.

Gestion des hôtes de conteneur

Vous pouvez afficher et gérer les hôtes que vous ajoutez depuis Hôtes. Dans le contexte de Conteneurs, l'hôte est une machine virtuelle ou une infrastructure qui vous permet d'exécuter des conteneurs.

L'onglet Hôtes réunit les contrôles permettant d'ajouter de nouveaux hôtes, de contrôler l'état des demandes de provisionnement des hôtes existants, de consulter les journaux d'événements de vos conteneurs et de procéder à la collecte de données sur les hôtes. Les volets Requêtes et Journal des événements sont situés à droite de la page.

Ajouter un hôte de conteneur

Vous devez ajouter un hôte pour déployer des conteneurs.

Lorsque vous ajoutez ou créez des hôtes dans Conteneurs, vous pouvez cliquer sur l'un des quatre panneaux de droite pour ajouter des options supplémentaires aux barres d'outils. Vous pouvez ajouter ou gérer des zones de placement, des informations d'identification, des certificats et des stratégies de déploiement.

Procédure

- 1 Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de conteneur**.
- 2 Cliquez sur l'onglet **Conteneurs**.
- 3 Cliquez sur **Ajouter un hôte**.
- 4 Entrez votre adresse IP hôte ou nom d'hôte au format **http(s)://<nomhôte>:<port>**.
- 5 Sous **Type d'hôte**, indiquez si vous avez entré l'adresse d'un hôte Docker ou d'un hôte de conteneur virtuel (VCH).
- 6 Sélectionnez vos informations d'identification pour la connexion dans la liste/
Conteneurs prend en charge l'authentification des identifiants de connexion et l'authentification par clé privée/publique.
- 7 Cliquez sur **Vérifier** pour confirmer la validité des paramètres configurés.
Une fois la vérification effectuée, de nouvelles zones de texte s'affichent dans lesquelles vous pouvez ajouter des informations complémentaires.
- 8 (Facultatif) Sélectionnez une zone de placement dans la liste.

Remarque Si vous configurez un VCH, la zone de placement et le placement sont automatiquement créés et connectés à l'hôte.

- 9 (Facultatif) Sélectionnez une stratégie de déploiement dans la liste.
- 10 (Facultatif) Définissez des propriétés personnalisées pour l'hôte.
- 11 Cliquez sur **Ajouter**.

Vous avez ajouté avec succès un hôte à Conteneurs.

Suivant

[Créer et gérer des positionnements de conteneur et des zones de positionnement](#)

Utilisation de stratégies de déploiement de conteneur

Vous pouvez lier des stratégies de déploiement à des hôtes et à des définitions de conteneur. Utilisez les stratégies de déploiement dans Conteneurs pour vRealize Automation pour définir une préférence pour l'hôte spécifique, ainsi que des quotas lorsque vous déployez un conteneur.

Les stratégies de déploiement qui sont appliqués à un conteneur ont une priorité plus élevée que les positionnements qui sont appliqués à des hôtes de conteneur.

Créer et gérer des positionnements de conteneur et des zones de positionnement

Vous pouvez utiliser des positionnements et des zones de positionnement pour limiter et réserver les ressources utilisées par un groupe d'activité. Vous pouvez également définir une priorité sur la quantité de mémoire réservée.

Vous pouvez modifier ou supprimer les positionnements que vous avez créés en les pointant puis en cliquant sur le bouton correspondant.

Lorsque vous créez ou gérez des positionnements, vous pouvez cliquer sur le bouton **Zones de positionnement** à droite pour ajouter ou gérer des zones de positionnement.

Remarque Si vous avez configuré un VCH, le positionnement et la zone de positionnement sont configurés automatiquement et ne peuvent pas être modifiés. Vous devez attribuer un groupe d'activité au positionnement, en cliquant sur l'icône **Modifier**.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de conteneur**.
- Assurez-vous que les ressources de mémoire spécifiées sont disponibles.
- Assurez-vous qu'au moins l'un des hôtes est configuré et disponible pour la configuration réseau des conteneurs.

Procédure

- 1 Cliquez sur l'onglet **Conteneurs**.
- 2 Cliquez sur **Positionnements**.
- 3 Cliquez sur **Ajouter**.
- 4 Entrez le nom de votre positionnement.
- 5 Attribuez le positionnement à un groupe d'activité.
- 6 Sélectionnez une zone de positionnement dans la liste.
- 7 Sélectionnez une stratégie de déploiement dans la liste.

- 8 (Facultatif) Entrez la valeur de priorité du positionnement.

Entrez un nombre positif, **1** représentant la priorité la plus élevée. Pour spécifier la priorité la moins élevée, laissez le champ vierge.

- 9 Spécifiez le nombre d'instances.

- 10 Sélectionnez la quantité de mémoire maximale pouvant être utilisée.

Sélectionnez un nombre compris entre 0 et la quantité de mémoire disponible dans la zone de positionnement. Il s'agit de la mémoire totale disponible pour les ressources dans ce positionnement. Pour ne spécifier aucune limite, entrez 0.

- 11 Cliquez sur **Enregistrer**.

Définir une stratégie de déploiement sur un hôte

Configurez une préférence pour l'hôte spécifique, ainsi que des quotas lorsque vous déployez un conteneur.

Procédure

- 1 Créez ou modifiez un hôte de conteneur.
- 2 Cliquez sur **Stratégies de déploiement** dans la partie droite pour développer une barre d'outils avec des options supplémentaires.
- 3 Cliquez sur **Ajouter** et donnez un nom et une description à la stratégie de déploiement.
- 4 Dans la vue **Ajouter hôte** ou **Modifier hôte**, sélectionnez la stratégie dans le menu déroulant **Stratégies de déploiement**.

Définir une stratégie de déploiement pour un positionnement

Définissez une stratégie de déploiement pour la configuration d'un positionnement.

Prérequis

Procédure

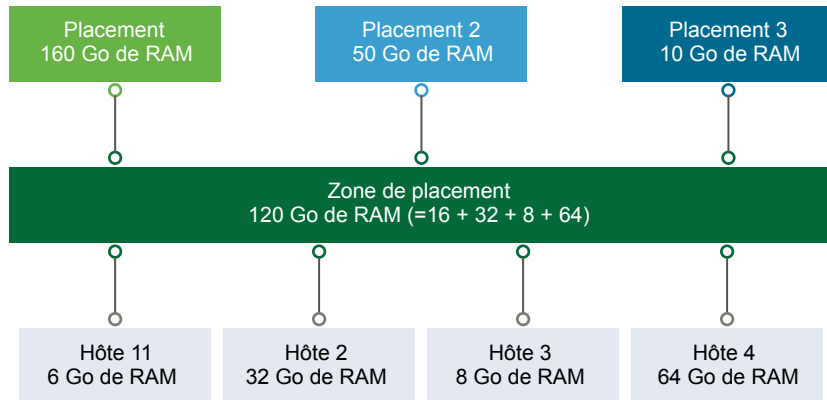
- 1 Cliquez sur l'onglet **Conteneurs**.
- 2 Cliquez sur **Positionnements**.
- 3 Déplacez le curseur sur un positionnement et cliquez sur l'icône **Modifier**.
- 4 Dans la liste déroulante **Stratégie de déploiement**, sélectionnez une stratégie existante.

Cette liste déroulante inclut également des contrôles pour rechercher une stratégie, créer une stratégie et gérer les stratégies. Vous pouvez également cliquer sur l'icône **Stratégie de déploiement** dans la partie droite de la page de positionnements pour accéder aux contrôles pour configurer les stratégies.
- 5 Cliquez sur **Enregistrer**.

Utilisation de zones de positionnement de conteneur

Une zone de positionnement est un ensemble d'hôtes, et les ressources disponibles dans une zone de positionnement sont la somme de toutes les ressources des hôtes qu'elle contient. Chaque positionnement est attribué à une zone de positionnement dans Conteneurs pour vRealize Automation. Plusieurs positionnements peuvent gérer une zone de positionnement unique.

Les positionnements qui gèrent une zone de positionnement ne peuvent pas réserver collectivement plus de ressources que celles qui sont disponibles dans le pool.



Lorsqu'un conteneur est provisionné, les positionnements sont filtrés en fonction du groupe d'activité, des ressources disponibles et de la priorité.

Configurer des paramètres de conteneur

Vous pouvez définir un conteneur unique ou une application à plusieurs conteneurs en utilisant les propriétés et les paramètres de conteneurs, nouveaux comme existants.

En supplément des paramètres clés de Conteneurs pour vRealize Automation, les paramètres vRealize Automation suivants sont disponibles pour les déploiements qui utilisent les composants de conteneur :

- Configuration de santé
- Liens
- Services exposés
- Taille de cluster et paramètres de réduction/montée en charge

Configurer les contrôles de santé dans Conteneurs

Vous pouvez configurer une méthode de contrôle de santé pour mettre à jour le statut d'un conteneur en fonction de critères personnalisés.

Vous pouvez utiliser des protocoles HTTP ou TCP lors de l'exécution d'une commande portant sur un conteneur. Vous pouvez également spécifier une méthode de contrôle de santé.

Prérequis

- Vérifiez que Conteneurs pour vRealize Automation est activé dans votre déploiement vRealize Automation pris en charge.
- Vous devez disposer de privilèges de rôle de type **administrateur de conteneur** ou **architecte de conteneur**.

Procédure

- 1 Connectez-vous à vRealize Automation.
- 2 Cliquez sur l'onglet **Conteneurs**.
- 3 Cliquez sur **Modèles** dans le panneau de gauche.
- 4 Modifiez le modèle ou l'image.

Option	Description
Pour modifier un modèle	<ul style="list-style-type: none"> ■ Cliquez sur Modifier dans la section supérieure droite du modèle à ouvrir. ■ Si le modèle recouvre plusieurs autres modèles, pointez sur le modèle que vous souhaitez modifier et cliquez sur Modifier dans la section supérieure droite du modèle que vous souhaitez ouvrir.
Pour modifier une image.	Cliquez sur la flèche près du bouton Provisionner de l'image et cliquez sur Entrer des informations supplémentaires .

- 5 Cliquez sur l'onglet **Configuration santé**.
- 6 Sélectionnez un mode de santé.

Tableau 2-20. Mode de configuration de l'état de santé

Mode	Description
Aucun	Par défaut. Aucun contrôle de santé n'est configuré.
HTTP	<p>Si vous sélectionnez HTTP, vous devez fournir une API d'accès, ainsi qu'une méthode et une version HTTP à utiliser. L'API est relative et il est superflu d'entrer l'adresse du conteneur. Vous pouvez également spécifier une période de délai d'attente pour l'opération et définir des seuils de santé.</p> <p>Par exemple, un seuil de santé ayant la valeur 2 signifie que deux appels réussis consécutifs doivent se produire pour que le conteneur soit considéré comme sain et passer à l'état EN COURS D'EXÉCUTION. Un seuil de défectuosité ayant la valeur 2 signifie que deux appels non-réussis consécutifs doivent se produire pour que le conteneur soit considéré comme défectueux et passer à l'état ERREUR. Pour tous les états intermédiaires, l'état du conteneur devient DÉTÉRIORÉ.</p>

Tableau 2-20. Mode de configuration de l'état de santé (suite)

Mode	Description
Connexion TCP	Si vous sélectionnez Connexion TCP , vous ne devez entrer que le port du conteneur. Le contrôle de santé tente d'établir une connexion TCP avec le conteneur sur le port fourni. Vous pouvez également spécifier une valeur de délai d'attente pour l'opération et définir des seuils de santé et de défectuosité comme pour l'option HTTP.
Commande	Si vous sélectionnez Commande , vous devez entrer une commande à exécuter sur le conteneur. Le succès du contrôle de santé est déterminé par l'état de sortie de la commande.
Ignorer le contrôle de santé lors du provisionnement	Décochez cette option pour forcer le contrôle de santé lors du provisionnement. Si ce contrôle est forcé, un conteneur n'est pas considéré comme étant provisionné tant qu'un contrôle de santé n'a pas réussi.
Autodeploy	Redéploiement automatique des conteneurs présentant l'état ERREUR.

- 7 Cliquez sur **Enregistrer comme modèle** pour enregistrer les paramètres, ou sélectionnez un groupe d'activité et cliquez sur **Provisionner** pour déployer le conteneur.

Configurer des liens dans Conteneurs

Communication des liens et des adresses de services exposés entre les services de conteneurs et équilibrage de charge entre les hôtes. Vous pouvez configurer les paramètres de liaison de vos conteneurs dans Conteneurs.

Vous pouvez également utiliser des liens pour activer la communication entre plusieurs services dans votre application. Les liens de Conteneurs sont similaires à ceux de Docker, mais ils connectent les conteneurs entre les différents hôtes. Un lien comprend deux parties : un nom de service et un alias. Le nom de service est le nom du service ou du modèle en cours d'appel. L'alias est le nom d'hôte que vous utilisez pour communiquer avec ce service.

Par exemple, si vous avez une application qui contient un service Web et un service de base de données, et si vous définissez un lien dans le service Web vers le service de base de données en utilisant l'alias `my-db`, l'application du service Web ouvre une connexion TCP vers `my-db: {PORT_OF_DB}`. La valeur `PORT_OF_DB` désigne le port écouté par la base de données, quel que soit le port public qui est affecté à l'hôte par les paramètres du conteneur. Si MySQL recherche des mises à jour sur son port par défaut, 3306, et si le port publié de l'hôte de conteneur est 32799, l'application Web accède à la base de données sur `my-db: 3306`.

Remarque Il est recommandé d'utiliser des réseaux plutôt que des liens. Les liens constituent désormais une fonctionnalité ancienne de Docker, avec des limitations significatives lors de la liaison de clusters de conteneurs, ce qui inclut :

- Docker ne prend pas en charge les liens multiples utilisant le même alias. Il est recommandé d'autoriser Conteneurs pour vRealize Automation à générer des alias de liens à votre place.
- Vous ne pouvez pas mettre à jour les liens d'une exécution de conteneur. Lors de la montée ou baisse en puissance d'un cluster lié, les liens du conteneur dépendant ne seront pas mis à jour.

Prérequis

- Vérifiez que Conteneurs pour vRealize Automation est activé dans votre déploiement vRealize Automation pris en charge.
- Vous devez disposer de privilèges de rôle de type **administrateur de conteneur** ou **architecte de conteneur**.
- Assurez-vous qu'un réseau bridgé est disponible pour lier les services.
- Assurez-vous également que le port interne du service cible est publié. Pour l'intercommunication, le service peut être mappé à tout autre port, mais doit être accessible en dehors de l'hôte.
- Vérifiez que les hôtes de service peuvent accéder l'un à l'autre.

Procédure

- 1 Connectez-vous à vRealize Automation.
- 2 Cliquez sur l'onglet **Conteneurs**.
- 3 Cliquez sur **Modèles** dans le panneau de gauche.
- 4 Modifiez le modèle ou l'image.

Option	Description
Pour modifier un modèle	<ul style="list-style-type: none"> ■ Cliquez sur Modifier dans la section supérieure droite du modèle à ouvrir. ■ Si le modèle recouvre plusieurs autres modèles, pointez sur le modèle que vous souhaitez modifier et cliquez sur Modifier dans la section supérieure droite du modèle que vous souhaitez ouvrir.
Pour modifier une image.	Cliquez sur la flèche près du bouton Provisionner de l'image et cliquez sur Entrer des informations supplémentaires .

5 Pour modifier un modèle

- a Cliquez sur **Modifier** dans la section supérieure droite du modèle à ouvrir.
- b Si le modèle recouvre plusieurs autres modèles, pointez sur le modèle que vous souhaitez modifier et cliquez sur **Modifier** dans la section supérieure droite du modèle que vous souhaitez ouvrir.

6 Pour modifier une image.

- a Cliquez sur la flèche près du bouton **Provisionner** de l'image et cliquez sur **Entrer des informations supplémentaires**.

La page **Provisionner un conteneur** ou **Modifier la définition de conteneur** s'affiche et donne accès à des ensembles hiérarchisés de propriétés et paramètres modifiables.

7 Cliquez sur l'onglet **Basique**.**8** Dans la zone de texte **Services**, entrez la liste des services dont le conteneur dépend en les séparant par des virgules.**9** Dans la zone de texte **Alias**, entrez un nom descriptif pour le service ou une liste de services séparés par une virgule.**10** Cliquez sur **Enregistrer**.**Configurer les services exposés dans Conteneurs**

Vous pouvez utiliser un nom d'hôte unique pour l'équilibrage de charge en fournissant une adresse et un espace réservé dans vos paramètres de conteneur.

L'emplacement réservé détermine l'emplacement d'une partie de l'URL qui est générée automatiquement. Cette valeur est unique pour chaque nom d'hôte. L'adresse prend en charge le caractère de mise en forme %, afin de spécifier l'emplacement réservé.

Remarque En l'absence d'emplacement réservé, l'adresse est positionnée en tant que préfixe ou suffixe du nom d'hôte, selon la configuration du système.

Il est recommandé d'utiliser un équilibrage de charge permettant de cibler les demandes pour chaque nœud si vous créez une application incluant un service devant être exposé publiquement et devant également réduire/monter en charge. Une fois l'application provisionnée, la configuration d'équilibrage de charge est mise à jour dès que la charge du service est réduite ou augmentée par vRealize Automation.

Prérequis

- Vérifiez que Conteneurs pour vRealize Automation est activé dans votre déploiement vRealize Automation pris en charge.
- Vous devez disposer de privilèges de rôle de type **administrateur de conteneur** ou **architecte de conteneur**.

Procédure**1** Connectez-vous à vRealize Automation.

- 2 Cliquez sur l'onglet **Conteneurs**.
- 3 Cliquez sur **Modèles** dans le panneau de gauche.
- 4 Modifiez le modèle ou l'image.

Option	Description
Pour modifier un modèle	<ul style="list-style-type: none"> ■ Cliquez sur Modifier dans la section supérieure droite du modèle à ouvrir. ■ Si le modèle recouvre plusieurs autres modèles, pointez sur le modèle que vous souhaitez modifier et cliquez sur Modifier dans la section supérieure droite du modèle que vous souhaitez ouvrir.
Pour modifier une image.	Cliquez sur la flèche près du bouton Provisionner de l'image et cliquez sur Entrer des informations supplémentaires .

- 5 Cliquez sur l'onglet **Réseau**.
- 6 Dans la zone de texte **Adresse**, entrez la position de l'emplacement réservé.
L'hôte d'adresse sert d'hôte virtuel. Pour accéder à l'hôte d'adresse, vous pouvez ajouter des informations de mappage dans le fichier etc/hosts ou utiliser un DNS qui mappe l'adresse du conteneur au nom d'hôte.
- 7 Dans la zone de texte **Port de conteneur**, entrez le numéro de port utilisé pour exposer le service.
Utilisez l'exemple de format fourni dans le formulaire. Si votre application de conteneur expose plusieurs ports, spécifiez le ou les ports internes pouvant exposer le service.
- 8 Cliquez sur **Enregistrer**.

Configurer la taille et le dimensionnement du cluster dans Conteneurs

Vous pouvez créer des clusters de conteneurs en utilisant les paramètres de positionnement de Conteneurs pour spécifier la taille de cluster.

Lorsque vous configurez un cluster, Conteneurs provisionne le nombre spécifié de conteneurs. Les charges de la demande sont équilibrées entre tous les conteneurs du cluster.

Vous pouvez modifier la taille de cluster d'un conteneur provisionné ou d'une application pour augmenter ou réduire individuellement la taille des clusters. Lorsque vous modifiez la taille des clusters pendant l'exécution, tous les filtres d'affinité et toutes les règles de positionnement sont pris en compte.

Prérequis

- Vérifiez que Conteneurs pour vRealize Automation est activé dans votre déploiement vRealize Automation pris en charge.
- Vous devez disposer de privilèges de rôle de type **administrateur de conteneur** ou **architecte de conteneur**.

Procédure

- 1 Connectez-vous à vRealize Automation.
- 2 Cliquez sur l'onglet **Conteneurs**.

- 3 Cliquez sur **Modèles** dans le panneau de gauche.
- 4 Modifiez le modèle ou l'image.

Option	Description
Pour modifier un modèle	<ul style="list-style-type: none"> ■ Cliquez sur Modifier dans la section supérieure droite du modèle à ouvrir. ■ Si le modèle recouvre plusieurs autres modèles, pointez sur le modèle que vous souhaitez modifier et cliquez sur Modifier dans la section supérieure droite du modèle que vous souhaitez ouvrir.
Pour modifier une image.	Cliquez sur la flèche près du bouton Provisionner de l'image et cliquez sur Entrer des informations supplémentaires .

- 5 Cliquez sur l'onglet **Stratégie**.
- 6 Définissez la taille du cluster du conteneur.
- 7 Enregistrez le modèle ou provisionnez-le.

Option	Description
Lorsque vous modifiez un modèle	Cliquez sur Enregistrer .
Lorsque vous modifiez une image	<ol style="list-style-type: none"> a Sélectionnez un groupe d'activité. b Cliquez sur Enregistrer comme modèle pour enregistrer les paramètres ou Provisionner pour déployer le conteneur.

Configuration et utilisation de modèles et d'images dans Conteneurs

Conteneurs utilise des modèles pour provisionner les conteneurs.

Un modèle est une configuration réutilisable pour provisionner un conteneur ou un ensemble de conteneurs. Dans un modèle, vous pouvez définir une application à plusieurs niveaux constituée de services liés.

Un service est défini comme un ou plusieurs conteneurs du même type ou image.

Vous pouvez créer un modèle de conteneur personnalisé basé sur un modèle existant sur la page **Modèles** ou importer un fichier YAML formaté correctement. Vous pouvez également provisionner un modèle ou une image de conteneur.

Créer un modèle de conteneur personnalisé

Vous pouvez créer un modèle personnalisé et l'utiliser pour définir un conteneur.

Un modèle est une configuration réutilisable que vous pouvez utiliser pour provisionner un conteneur ou une suite de conteneurs.

La page Modèles affiche des images de modèle qui sont mises à votre disposition sur la base des registres que vous avez définis. Vous pouvez créer un modèle personnalisé reposant sur une image de modèle existante ou importer un modèle, ou encore un fichier Docker Compose. Reportez-vous à [Importer un modèle de conteneur ou un fichier Docker Compose](#).

Vous pouvez également créer un modèle ou une image personnalisée en utilisant l'option **Provisionner > Entrer des informations supplémentaires** décrite dans [Provisionner un conteneur à partir d'un modèle ou d'une image](#).

Prérequis

- Vous devez disposer de privilèges de rôle de type **administrateur de conteneur**.

Procédure

- 1 Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de conteneur**.
- 2 Cliquez sur l'onglet **Conteneurs**.
- 3 Cliquez sur **Modèles** dans le panneau de gauche.

Une liste affiche les modèles et les images qui sont disponibles pour le provisionnement.

- Modèles configurés dans la vue Images.
- Modèles existants ou personnalisés dans la vue **Modèle**.
- Tous les modèles et les images disponibles basés sur les registres que vous avez spécifié dans la vue **Tout**.

Les options **Importer** et **Exporter** sont également disponibles, afin d'importer ou exporter des modèles et des images.

- 4 Cliquez sur la flèche en regard du bouton **Provisionner** d'une image à inclure dans le modèle.
- 5 Cliquez sur **Entrer des informations complémentaires**.
- 6 Cliquez sur **Enregistrer comme modèle** pour enregistrer vos modifications en tant que nouveau modèle de conteneur dans des conteneurs pour vRealize Automation.

Suivant

Vous pouvez provisionner un modèle en prévision des provisionnements futurs. Les applications existantes qui ont été provisionnées depuis le modèle ne sont pas affectées par les modifications que vous apportez au modèle après le provisionnement.

Importer un modèle de conteneur ou un fichier Docker Compose

Vous pouvez utiliser un modèle de conteneur du Docker importé ou un fichier YAML Docker Compose en tant que modèle personnalisé dans Conteneurs pour vRealize Automation?

Si vous utilisez un fichier YAML, entrez le contenu de ce fichier au format texte ou recherchez et téléchargez le fichier YAML. Le fichier YAML représente le modèle, la configuration des différents conteneurs et leurs connexions. Les types de format pris en charge sont YAML Docker Compose et YAML Conteneurs pour vRealize Automation.

Le format YAML Conteneurs pour vRealize Automation est similaire au format Docker Compose, mais il utilise le format YAML de Blueprint vRealize Automation visible dans l'API REST vRealize Automation ou dans vRealize CloudClient. Le format YAML Conteneurs pour vRealize Automation vous permet d'importer les applications Docker Compose existantes et de les modifier, provisionner et gérer à l'aide de Conteneurs.

Prérequis

- Vérifiez que Conteneurs pour vRealize Automation est activé dans votre déploiement vRealize Automation pris en charge.
- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de conteneur**.

Pour plus d'informations sur le format YAML par les API REST du service vRealize Automation, reportez-vous à *Référence de l'API de vRealize Automation*.

Procédure

1 Cliquez sur l'onglet **Conteneurs**.

2 Cliquez sur **Modèles** dans le panneau de gauche.

Une liste affiche les modèles et les images qui sont disponibles pour le provisionnement.

- Modèles configurés dans la vue Images.
- Modèles existants ou personnalisés dans la vue **Modèle**.
- Tous les modèles et les images disponibles basés sur les registres que vous avez spécifié dans la vue **Tout**.

Les options **Importer** et **Exporter** sont également disponibles, afin d'importer ou exporter des modèles et des images.

3 Cliquez sur l'icône **Importer modèle ou Docker Compose**.

La page Importer modèle s'affiche.

4 Fournissez le contenu de fichier YAML.

Option	Description
Charger depuis fichier	Cliquez sur Charger depuis fichier afin de parcourir et sélectionner les fichiers YAML depuis un répertoire.
Entrer modèle ou Docker Compose	Collez le contenu d'un fichier YAML correctement formaté dans la zone de texte Entrer modèle ou Docker Compose .

5 Cliquez sur **Importer**.

Le nouveau modèle s'affiche dans la vue **Modèles**.

Provisionner un conteneur à partir d'un modèle ou d'une image

Vous pouvez provisionner un conteneur à partir d'un modèle ou d'une image dans la vue Modèles.

Le processus de provisionnement crée un conteneur basé sur les paramètres de configuration qui existent dans le modèle ou l'image à partir duquel vous le provisionnez.

Vous pouvez provisionner un conteneur à partir d'un modèle ou d'une image en utilisant les paramètres de configuration existants ou en les modifiant avant de le provisionner.

Vous pouvez également modifier et enregistrer les paramètres de configuration pour créer un nouveau modèle ou image de conteneur personnalisé.

Prérequis

- Vérifiez que Conteneurs pour vRealize Automation est activé dans votre déploiement vRealize Automation pris en charge.
- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de conteneur**.

Procédure

1 Cliquez sur l'onglet **Conteneurs**.

2 Cliquez sur **Modèles** dans le panneau de gauche.

Une liste affiche les modèles et les images qui sont disponibles pour le provisionnement.

- Modèles configurés dans la vue Images.
- Modèles existants ou personnalisés dans la vue **Modèle**.
- Tous les modèles et les images disponibles basés sur les registres que vous avez spécifié dans la vue **Tout**.

Les options **Importer** et **Exporter** sont également disponibles, afin d'importer ou exporter des modèles et des images.

3 Pour afficher l'image ou le modèle à provisionner, utilisez les options de la vue **Tout**, **Images** ou **Modèles**.

4 Provisionnez le modèle ou l'image de conteneur.

Option	Description
Provisionner en utilisant les paramètres existants.	<p>a Cliquez sur Provisionner.</p> <p>La vue Demandes de provisionnement affiche les informations sur la réussite du provisionnement.</p>
Provisionner en modifiant les paramètres.	<p>a Cliquez sur la flèche en regard du bouton Provisionner.</p> <p>b Cliquez sur Entrer des informations complémentaires.</p> <p>c Entrez les informations complémentaires pour le conteneur dans le formulaire Provisionner un conteneur.</p> <p>d Lorsque vous avez mis à jour le formulaire, cliquez sur Provisionner pour provisionner le conteneur en utilisant les paramètres modifiés.</p> <p>e Cliquez sur Enregistrer comme modèle pour enregistrer vos modifications en tant que nouveau modèle de conteneur dans Conteneurs pour vRealize Automation.</p> <p>La vue Demandes de provisionnement affiche les informations sur la réussite du provisionnement.</p>

Exporter un modèle de conteneur ou un fichier Docker Compose

Vous pouvez exporter un modèle de conteneur en tant que fichier YAML Docker Compose ou un fichier YAML Conteneurs pour vRealize Automation.

Vous pouvez importer un modèle et le modifier par programmation à l'aide de l'API REST vRealize Automation ou vRealize CloudClient, ou graphiquement dans Conteneurs. Vous pouvez ensuite exporter le fichier modifié. Par exemple, vous pouvez l'importer dans le format Docker Compose et l'exporter dans le format YAML de Blueprint utilisé dans l'API de composition de service vRealize Automation. Cependant, certaines configurations spécifiques à Conteneurs, comme la configuration de la santé et les contraintes d'affinité, ne sont pas incluses si vous exportez le modèle dans le format Docker Compose.

Prérequis

- Vérifiez que Conteneurs pour vRealize Automation est activé dans votre déploiement vRealize Automation pris en charge.
- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de conteneur**.

Pour plus d'informations sur le format YAML par les API REST du service vRealize Automation, reportez-vous à *Référence de l'API de vRealize Automation*.

Procédure

1 Cliquez sur l'onglet **Conteneurs**.

2 Cliquez sur **Modèles** dans le panneau de gauche.

Une liste affiche les modèles et les images qui sont disponibles pour le provisionnement.

- Modèles configurés dans la vue Images.
- Modèles existants ou personnalisés dans la vue **Modèle**.
- Tous les modèles et les images disponibles basés sur les registres que vous avez spécifié dans la vue **Tout**.

Les options **Importer** et **Exporter** sont également disponibles, afin d'importer ou exporter des modèles et des images.

3 Pointez vers un modèle et cliquez sur son icône **Exporter**.

4 Lorsque vous y êtes invité, sélectionnez un type de format de sortie :

- **Blueprint YAML**

Ce format respecte le format YAML de Blueprint utilisé dans l'API de composition de service vRealize Automation.

- **Docker Compose**

Ce format respecte le format YAML utilisé dans l'application Docker Compose.

5 Cliquez sur **Exporter**.

6 Enregistrez le fichier ou ouvrez-le avec une application appropriée lorsque vous y êtes invité.

Utilisation de registres de conteneur

Un registre du Docker est une application sans état côté serveur. Vous pouvez utiliser les registres dans les Conteneurs pour vRealize Automation pour stocker et distribuer des images du Docker.

Pour configurer un registre, vous devez fournir son adresse, un nom de registre personnalisé et éventuellement des informations d'identification. L'adresse doit commencer par HTTP ou HTTPS pour indiquer si le registre est sécurisé ou non. Si le type de connexion n'est pas fourni, HTTPS est utilisé par défaut.

Remarque Pour HTTP, vous devez déclarer le port 80 ; pour HTTPS, vous devez déclarer le port 443. Si aucun port n'est spécifié, le moteur du Docker attend le port 5000, qui peut entraîner des interruptions de connexion.

Remarque Il est recommandé de ne pas utiliser de registres HTTP, car le protocole HTTP est considéré comme n'étant pas sécurisé. Si vous souhaitez utiliser le HTTP, vous devez modifier la propriété DOCKER_OPTS sur chaque hôte de la manière suivante :

```
DOCKER_OPTS="--insecure-registry myregistrydomain.com:5000".
```

Pour plus d'informations, reportez-vous à la documentation de Docker sur <https://docs.docker.com/registry/insecure/>.

Conteneurs peut interagir avec l'API HTTP de registre du Docker V1 et V2 de la manière suivante :

V1 sur HTTP (non sécurisé, registre HTTP brut)

Vous pouvez rechercher ce type de registre librement, mais vous devez configurer manuellement chaque hôte du Docker avec la balise `--insecure-registry` pour provisionner des images basées sur des conteneurs provenant de registres non sécurisés. Après avoir défini la propriété, vous devez redémarrer le démon du Docker.

V1 sur HTTPS

Utilisez cette API derrière un proxy inverse, comme NGINX. La mise en œuvre standard est disponible en version libre à l'adresse <https://github.com/docker/docker-registry>.

V2 sur HTTPS

La mise en œuvre standard est disponible en version libre à l'adresse <https://github.com/docker/distribution>.

V2 sur HTTPS avec authentification de base

La mise en œuvre standard est disponible en version libre à l'adresse <https://github.com/docker/distribution>.

V2 sur HTTPS avec authentification par le biais d'un service central

Vous pouvez exécuter un registre du Docker en mode autonome, dans lequel il n'y a pas de contrôles des autorisations. Les registres tiers pris en charge sont JFrog Artifactory et Harbor. Le hub du Docker est activé par défaut pour tous les locataires et n'est pas présent dans la liste des registres, mais il peut être désactivé avec une propriété système.

Remarque Normalement, le Docker n'interagit pas avec les registres sécurisés configurés avec des certificats signés par une autorité inconnue. Le service de conteneurs gère cette situation en téléchargeant automatiquement des certificats non autorisés sur tous les hôtes du Docker et en autorisant les hôtes à se connecter à ces registres. Si un certificat ne peut pas être téléchargé sur un hôte spécifique, l'hôte est désactivé automatiquement.

Créer et gérer des registres de conteneurs

Vous pouvez configurer plusieurs registres pour accéder à des images publiques et privées.

Les registres sont des magasins publics ou privés à partir desquels vous chargez ou téléchargez des images. Vous pouvez désactiver, modifier ou supprimer les registres que vous avez créés. Les images qui s'affichent dans l'onglet **Modèles** sont basées sur les registres que vous définissez.

Lorsque vous créez ou gérez des registres sur la page Registres existants, vous pouvez cliquer sur les boutons **Informations d'identification** ou **Certificat** pour ajouter ou gérer des informations d'identification et des certificats.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de conteneur**.
- Assurez-vous qu'au moins l'un des hôtes est configuré et disponible pour la configuration réseau des conteneurs.

Procédure

- 1 Cliquez sur l'onglet **Conteneurs**.
- 2 Cliquez sur **Modèles**.
- 3 Cliquez sur **Gérer un registre**.
La page Registres existants s'affiche.
- 4 Cliquez sur **Ajouter**.
- 5 Entrez l'adresse du registre.
- 6 Entrez le nom du registre.
- 7 Sélectionnez vos informations de connexion dans la liste déroulante.
- 8 (Facultatif) Cliquez sur **Vérifier** pour confirmer la validité des paramètres configurés.

- 9 Cliquez sur **Enregistrer** pour ajouter le Registre.

Configuration des ressources réseau pour les conteneurs

Vous pouvez créer, modifier et attacher des configurations réseau aux conteneurs et aux modèles de conteneur dans l'application Conteneurs pour vRealize Automation.

Lorsque vous provisionnez un conteneur, la configuration du réseau est intégrée et disponible. Vous pouvez personnaliser les paramètres réseau des composants de conteneur que vous avez ajoutés à un Blueprint vRealize Automation.

Créer un nouveau réseau pour les conteneurs

Si aucune configuration réseau adaptée n'est disponible, vous pouvez en créer une dans vRealize Automation.

Prérequis

- Assurez-vous que vous disposez de privilèges de rôle de type **administrateur de conteneur**, **architecte de conteneur** ou **administrateur IaaS**.
- Assurez-vous qu'au moins l'un des hôtes est configuré et disponible pour la configuration réseau des conteneurs.

Procédure

- 1 Connectez-vous à vRealize Automation.
- 2 Cliquez sur l'onglet **Conteneurs**.
- 3 Sélectionnez **Réseaux** dans le volet de gauche.

Le panneau principal affiche les configurations réseau existantes qui peuvent être provisionnées dans le cadre du déploiement du conteneur. Les configurations réseau incluent celles qui sont collectées depuis les hôtes Docker ajoutés et celles créées dans vRealize Automation. Les icônes représentant les configurations réseau affichent le réseau et les pilotes IPAM ; les informations de sous-réseau, de passerelle et de plage IP ; le nombre de conteneurs utilisant la configuration réseau ; puis le nombre d'hôtes.

- 4 Cliquez sur **Créer réseau**.
- 5 Entrez le nom du réseau.

Lorsque vous avez créé la nouvelle configuration, un identifiant unique est ajouté à la valeur du nom.

- 6 (Facultatif) Pour ajouter des paramètres de configuration plus détaillés, cochez la case **Avancé**.

Les paramètres de configuration réseau avancée s'affichent dans le panneau Ajouter réseau.

7 Configurez les paramètres de configuration de réseau avancées.

Option	Description
Configuration IPAM	<p>Sous-réseau</p> <p>Fournissez les adresses de sous-réseau et de passerelle propres à cette configuration réseau. Elles ne doivent chevaucher tout autre réseau dans le même hôte de conteneur.</p>
Propriétés personnalisées	<p>Vous pouvez spécifier des propriétés personnalisées pour la nouvelle configuration réseau.</p> <p>containers.ipam.driver</p> <p>À utiliser uniquement avec des conteneurs. Spécifie le pilote IPAM à utiliser lors de l'ajout d'un composant réseau Conteneurs à un Blueprint. Les valeurs prises en charge dépendent des pilotes installés dans l'environnement hôte des conteneurs dans lequel ils sont utilisés. Par exemple, une valeur prise en charge peut être <code>infoblox</code> ou <code>calico</code> selon les plug-ins IPAM qui sont installés sur l'hôte des conteneurs.</p> <p>Le nom et la valeur de cette propriété sont sensibles à la casse. La valeur de la propriété n'est pas validée lorsque vous l'ajoutez. Si le pilote spécifié n'existe pas sur l'hôte de conteneur au moment du provisionnement, un message d'erreur est renvoyé et le provisionnement échoue.</p> <p>containers.network.driver</p> <p>À utiliser uniquement avec des conteneurs. Spécifie le pilote réseau à utiliser lors de l'ajout d'un composant réseau Conteneurs à un Blueprint. Les valeurs prises en charge dépendent des pilotes installés dans l'environnement hôte des conteneurs dans lequel ils sont utilisés. Par défaut, les pilotes réseau fournis par le Docker incluent Bridge, Overlay et Macvlan, tandis que les pilotes réseau fournis par VCH (Virtual Container Host) incluent le pilote Bridge. Des pilotes réseau tiers tels que <code>weave</code> et <code>calico</code> peuvent également être disponibles, selon les plug-ins de mise en réseau installés sur l'hôte de conteneur.</p> <p>Le nom et la valeur de cette propriété sont sensibles à la casse. La valeur de la propriété n'est pas validée lorsque vous l'ajoutez. Si le pilote spécifié n'existe pas sur l'hôte de conteneur au moment du provisionnement, un message d'erreur est renvoyé et le provisionnement échoue.</p>

Remarque Si vous créez le réseau sans paramètres avancés, vRealize Automation fournit les paramètres automatiquement.

8 Dans le menu déroulant, sélectionnez l'hôte auquel vous souhaitez connecter le réseau.

9 Cliquez sur **Créer**.

Ajouter un réseau à un modèle de conteneur

Vous pouvez ajouter une configuration réseau à un modèle de conteneur, afin de connecter les conteneurs entre eux. Cette configuration réseau est automatiquement mise en œuvre pour toutes les applications qui utilisent le modèle. Vous pouvez ajouter un réseau existant, ou configurer et ajouter un nouveau réseau en fonction des besoins.

Prérequis

- Assurez-vous qu'un modèle est disponible. Sinon, vous devez en créer un.
- Assurez-vous que vous disposez de privilèges de rôle de type **administrateur de conteneur**, **architecte de conteneur** ou **administrateur IaaS**.
- Assurez-vous qu'au moins l'un des hôtes est configuré et disponible pour la configuration réseau des conteneurs.

Procédure

- 1 Connectez-vous à vRealize Automation.
- 2 Cliquez sur l'onglet **Conteneurs**.
- 3 Cliquez sur **Modèles** dans le panneau de gauche.
Un groupe d'icônes affiche les modèles et les images qui sont disponibles pour le provisionnement.
- 4 (Facultatif) Modifiez la vue, afin d'afficher uniquement les modèles en cliquant sur **Afficher : Modèles** dans l'en-tête supérieur droit, au-dessus des icônes.
- 5 Cliquez sur **Modifier** dans la section supérieure droite du modèle à personnaliser.
La page Modifier le modèle s'affiche et inclut les icônes de conteneur, ainsi qu'une icône vide et un signe plus.
- 6 Pointez l'icône vide.
L'icône **Ajouter un réseau** s'affiche.
- 7 Cliquez sur l'icône **Ajouter réseau**.
Le panneau Ajouter un réseau s'affiche.
- 8 Ajoutez un réseau existant ou créez et ajoutez un nouveau réseau.

Option	Description
Ajouter un réseau existant	<ol style="list-style-type: none"> a Cochez la case Réseau existant. b Cliquez dans le champ Nom pour afficher une liste des réseaux existants. c Sélectionnez le réseau que vous souhaitez utiliser, puis cliquez sur Enregistrer.
Configurer et ajouter un nouveau réseau	<ol style="list-style-type: none"> a Entrez le nom du réseau. b Pour ajouter des paramètres de configuration plus détaillés, cochez la case Avancé. c Cliquez sur Enregistrer.

Le panneau Ajouter une configuration réseau disparaît et le réseau ajouté s'affiche sous forme d'icône horizontale en dessous des icônes de conteneur sur la page Modifier le modèle. Une icône de réseau s'affiche également sur la bordure inférieure des icônes de conteneur.

- 9 Connectez le réseau à un conteneur en faisant glisser l'icône de connecteur réseau du conteneur vers un point quelconque de l'icône horizontale représentant le réseau.

Configuration de volumes pour les conteneurs

Vous pouvez créer, modifier et attacher des volumes aux conteneurs et aux modèles de conteneur dans l'application Conteneurs pour vRealize Automation.

Conteneurs pour vRealize Automation utilise des volumes de Docker pour la gestion des données persistantes. Les volumes vous permettent d'effectuer les tâches suivantes :

- Partager des volumes entre différents conteneurs dans le même hôte.
- Mettre à jour des données instantanément.
- Enregistrer les données de volume après avoir supprimé le conteneur.

Créer un volume pour les conteneurs

Pour étendre votre stockage de conteneur, vous devez d'abord créer un volume de données.

Prérequis

- Assurez-vous que vous disposez de privilèges de rôle de type **administrateur de conteneur**, **architecte de conteneur** ou **administrateur IaaS**.
- Assurez-vous qu'au moins l'un des hôtes est configuré et disponible pour la configuration du volume de conteneur.

Procédure

- 1 Connectez-vous à vRealize Automation.
- 2 Cliquez sur l'onglet **Conteneurs**.
- 3 Sélectionnez **Ressources > Réseaux** dans le panneau de gauche.

Le volet principal affiche les configurations de volume existantes qui peuvent être connectées aux conteneurs déployés. Les configurations de volume incluent celles qui sont collectées depuis les hôtes Docker ajoutés et celles créées dans vRealize Automation. Les instances de volume affichent le pilote, la portée et les options du pilote.

- 4 Cliquez sur **Créer un Volume**.
- 5 Entrez le nom du volume.

Une fois la configuration créée, un identifiant unique est ajouté à la valeur du nom.

- 6 Dans la zone de texte **Pilote**, entrez le pilote du plug-in Volume à utiliser. Si vous n'entrez rien, la valeur par défaut est « local ».

- 7 (Facultatif) Pour ajouter des paramètres de configuration plus détaillés, cochez la case **Avancé**.

Des paramètres de configuration supplémentaires s'affichent.

- 8 (Facultatif) Configurez les paramètres de volume avancés.

Option	Description
Options de pilote	Spécifiez les options de pilote que vous souhaitez utiliser. Les options varient selon le plug-in Volume que vous utilisez.
Propriétés personnalisées	Spécifiez des propriétés personnalisées pour la nouvelle configuration.

- 9 Dans le menu déroulant, sélectionnez l'hôte auquel vous souhaitez connecter le volume.

- 10 Cliquez sur **Créer**.

Le panneau de création de volume disparaît et le volume ajouté s'affiche dans l'onglet Volumes.

Suivant

[Ajouter un volume à un modèle de conteneur](#)

Ajouter un volume à un modèle de conteneur

Connectez un volume à un conteneur en l'ajoutant à un modèle.

Prérequis

- Assurez-vous qu'un modèle est disponible. Sinon, vous devez en créer un.
- Assurez-vous que vous disposez de privilèges de rôle de type **administrateur de conteneur**, **architecte de conteneur** ou **administrateur IaaS**.
- Assurez-vous qu'au moins l'un des hôtes est configuré et disponible pour la configuration du volume de conteneur.

Procédure

- 1 Connectez-vous à vRealize Automation.

- 2 Cliquez sur l'onglet **Conteneurs**.

- 3 Cliquez sur **Modèles** dans le panneau de gauche.

Un groupe d'icônes affiche les modèles et les images qui sont disponibles pour le provisionnement.

- 4 (Facultatif) Modifiez la vue, afin d'afficher uniquement les modèles en cliquant sur **Afficher : Modèles** dans l'en-tête supérieur droit, au-dessus des icônes.

- 5 Cliquez sur **Modifier** dans la section supérieure droite du modèle à personnaliser.

La page Modifier le modèle s'affiche et inclut les icônes de conteneur, ainsi qu'une icône vierge et un signe plus.

- 6 Déplacez le curseur sur l'icône vierge avec le signe plus jusqu'à ce que l'icône **Ajouter un volume** s'affiche.

- 7 Cliquez sur l'icône **Ajouter un volume**.

8 Ajoutez un volume existant ou créez et ajoutez un nouveau volume.

Option	Description
Ajouter un volume existant	<ul style="list-style-type: none"> a Cochez la case Réseau existant. b Cliquez dans le champ Nom pour afficher une liste des volumes existants. c Sélectionnez le volume que vous souhaitez utiliser, puis cliquez sur Enregistrer.
Configurer et ajouter un nouveau volume	<ul style="list-style-type: none"> a Entrez le nom du volume. b Dans la zone de texte Pilote, entrez le pilote du plug-in Volume à utiliser. Si vous n'utilisez pas un système de stockage externe, entrez local. c Pour ajouter des paramètres de configuration plus détaillés, cochez la case Avancé. d Cliquez sur Enregistrer.

Le panneau Ajouter un volume disparaît et le volume ajouté s'affiche sous forme d'icône horizontale en dessous des icônes de conteneur dans la page Modifier le modèle. Une icône de volume s'affiche également sur la bordure inférieure des icônes de conteneur.

- 9 Connectez le volume à un conteneur en faisant glisser l'icône de connecteur volume du conteneur vers un point quelconque de l'icône horizontale représentant le volume.
- 10 (Facultatif) Cliquez sur le chemin d'accès de conteneur pour modifier l'emplacement dans lequel le volume est monté.

Suivant

[Provisionner un conteneur à partir d'un modèle ou d'une image](#)

Installation de plug-ins supplémentaires sur le serveur vRealize Orchestrator par défaut

Vous pouvez installer des modules et des plug-ins sur le serveur vRealize Orchestrator par défaut en utilisant l'interface de configuration vRealize Orchestrator.

Vous pouvez installer des plug-ins supplémentaires sur le serveur vRealize Orchestrator par défaut et utiliser les workflows avec XaaS.

Vous pouvez également importer des modules supplémentaires sur le serveur vRealize Orchestrator par défaut pour une configuration comme types de point de terminaison de fournisseur IPAM externe vRealize Automation. Par exemple, pour obtenir des informations sur l'obtention, l'importation et la configuration du module Infoblox IPAM, reportez-vous à [Liste de contrôle pour assurer la prise en charge d'un fournisseur IPAM tiers](#).

Les fichiers de modules (.package) et les fichiers d'installation de plug-ins (.vmoapp ou .dar) sont disponibles dans VMware Solution Exchange à l'adresse https://solutionexchange.vmware.com/store/category_groups/cloud-management. Pour plus d'informations sur les fichiers de plug-ins, reportez-vous à la vRealize Orchestrator documentation sur les plug-ins à l'adresse https://www.vmware.com/support/pubs/vco_plugins_pubs.html.

Pour plus d'informations sur l'installation de nouveaux plug-ins, reportez-vous à la section *Installation et configuration de VMware vCenter Orchestrator*.

Utilisation de stratégies Active Directory

Les stratégies Active Directory définissent les propriétés d'un enregistrement de machine (par exemple, le domaine), ainsi que l'unité d'organisation dans laquelle l'enregistrement est créé à l'aide d'un Blueprint vRealize Automation.

Si vous appliquez une stratégie à un groupe d'activité, toutes les demandes de machines des membres du groupe d'activité sont ajoutées à l'unité d'organisation spécifiée. Vous pouvez créer différentes stratégies pour différentes unités d'organisation, puis appliquer les différentes stratégies à différents groupes d'activité.

Les stratégies Active Directory sont une fonctionnalité tech preview dans vRealize Automation 7.1 et ne doivent pas être utilisées dans un environnement de production.

Utilisation de propriétés personnalisées pour remplacer une stratégie Active Directory

À l'aide des propriétés personnalisées Active Directory fournies, vous pouvez remplacer la stratégie Active Directory, le domaine, l'unité d'organisation et d'autres valeurs sur un Blueprint particulier lors de son déploiement.

La liste des propriétés personnalisées Active Directory fournies est incluse dans le document *Référence des propriétés personnalisées*. Le préfixe de propriété personnalisée est `ext.policy.activedirectory`.

Outre les propriétés fournies, vous pouvez créer vos propres propriétés personnalisées. Vous devez utiliser le préfixe `ext.policy.activedirectory` avec vos propriétés personnalisées. Par exemple, `ext.policy.activedirectory.domain.extension` ou `ext.policy.activedirectory.yourproperty`. Les propriétés sont passées à vos workflows Active Directory de vRealize Orchestrator.

Pour plus d'informations sur les propriétés personnalisées, reportez-vous à *Référence des propriétés personnalisées*. Selon les valeurs que vous remplacez, vous devrez éventuellement créer une définition de propriété. Par exemple, vous pouvez créer une définition de propriété qui récupère les stratégies Active Directory disponibles de vRealize Automation. Vous pouvez également créer une définition qui permet à l'utilisateur demandeur de sélectionner plusieurs autres unités d'organisation. Reportez-vous à *Référence des propriétés personnalisées*.

Créer et appliquer des stratégies Active Directory

Vous créez une ou plusieurs stratégies Active Directory pour pouvoir attribuer différentes stratégies à différents groupes d'activité. Vous pouvez utiliser les stratégies différentes pour ajouter des enregistrements de machine à des unités d'organisation différentes en fonction de l'appartenance à un groupe d'activité.

Si nécessaire, vous pouvez remplacer la stratégie Active Directory attribuée.

Procédure

1 Créer une stratégie Active Directory

Vous créez une stratégie Active Directory pour définir où les enregistrements sont ajoutés dans une instance d'Active Directory lorsque vos utilisateurs déploient des machines. Vous pouvez attribuer une stratégie à un groupe d'activité pour que toutes les machines déployées par les membres du groupe d'activité entraînent la création d'un enregistrement dans l'unité d'organisation spécifiée.

2 Scénario : ajouter une propriété personnalisée à des Blueprints pour remplacer une stratégie Active Directory

En tant qu'architecte de Blueprints pour le groupe d'activité de développement, vous disposez d'un Blueprint qui inclut une machine d'application et une machine de base de données. Vous souhaitez que l'enregistrement de machine de base de données ajouté à une unité d'organisation soit différent de la stratégie Active Directory appliquée.

Créer une stratégie Active Directory

Vous créez une stratégie Active Directory pour définir où les enregistrements sont ajoutés dans une instance d'Active Directory lorsque vos utilisateurs déploient des machines. Vous pouvez attribuer une stratégie à un groupe d'activité pour que toutes les machines déployées par les membres du groupe d'activité entraînent la création d'un enregistrement dans l'unité d'organisation spécifiée.

Vous créez des stratégies Active Directory différentes lorsque vous souhaitez que les machines déployées par différents groupes d'activité aient des domaines différents ou soient ajoutées à des instances différentes d'Active Directory.

Prérequis

- Vérifiez que vous avez créé un point de terminaison Active Directory. Reportez-vous à [Configurer le plug-in Active Directory comme un point de terminaison](#).
- Si vous utilisez un serveur vRealize Orchestrator externe, assurez-vous qu'il est configuré correctement. Reportez-vous à [Configurer un serveur vRealize Orchestrator externe](#).
- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

1 Sélectionnez **Administration > Stratégies AD**.

2 Cliquez sur l'icône **Nouveau** (+).

3 Configurez les détails de la stratégie Active Directory.

Option	Description
ID	Entrez la valeur permanente. La valeur ne peut pas inclure d'espaces ou de caractères spéciaux. Vous ne pouvez pas modifier cette valeur ultérieurement. Vous pouvez uniquement recréer la stratégie avec un ID différent.
Description	Décrivez la stratégie.
Point de terminaison Active Directory	Sélectionnez le point de terminaison Active Directory pour lequel cette stratégie est créée.
Contrôleur	Entrez le domaine racine. Le format est <i>mycompany.com</i> .
Unité d'organisation	Entrez le nom unique de l'unité d'organisation pour cette stratégie. La hiérarchie doit être entrée sous la forme d'une liste séparée par des virgules. Par exemple, ou=development,dc=corp,dc=domain,dc=com.

4 Cliquez sur **OK**.

Le point de terminaison vRealize Orchestrator Active Directory est ajouté à la liste. Vous pouvez appliquer la stratégie dans des groupes d'activité ou utiliser la stratégie dans des Blueprints ou des groupes d'activité.

Suivant

- Pour fournir plusieurs options de stratégie, créez d'autres stratégies.
- Pour ajouter des enregistrements à Active Directory sur la base de l'appartenance à un groupe d'activité lorsqu'un Blueprint est déployé, ajoutez la stratégie Active Directory appropriée à un groupe d'activité. Reportez-vous à [Créer un groupe d'activité](#). Vous pouvez appliquer la stratégie lorsque vous créez le groupe d'activité ou vous pouvez l'ajouter ultérieurement.
- Pour remplacer la stratégie Active Directory pour le groupe d'activités d'un Blueprint particulier, ajoutez les propriétés personnalisées Active Directory au Blueprint. Reportez-vous à [Scénario : ajouter une propriété personnalisée à des Blueprints pour remplacer une stratégie Active Directory](#).

Scénario : ajouter une propriété personnalisée à des Blueprints pour remplacer une stratégie Active Directory

En tant qu'architecte de Blueprints pour le groupe d'activité de développement, vous disposez d'un Blueprint qui inclut une machine d'application et une machine de base de données. Vous souhaitez que l'enregistrement de machine de base de données ajouté à une unité d'organisation soit différent de la stratégie Active Directory appliquée.

Vous avez une stratégie existante qui est appliquée au groupe d'activité de développement. La stratégie ajoute des enregistrements à ou=development,dc=corp,dc=domain,dc=com. Vous souhaitez que toutes les machines de base de données soient ajoutées à ou=databases,dc=corp,dc=domain,dc=com. Dans un Blueprint incluant un serveur de base de données, vous remplacez l'unité d'organisation Active Directory pour ajouter la machine de base de données à ou=databases,dc=corp,dc=domain,dc=com.

Ce scénario repose sur les hypothèses suivantes :

- Votre annuaire Active Directory inclut des unités d'organisation pour le développement et les bases de données.
- Vous avez un Blueprint de test qui est inclus dans un service et ce dernier dispose d'une autorisation d'accès.

Outre cet exemple simple de remplacement de la stratégie, vous pouvez utiliser des propriétés personnalisées avec une stratégie Active Directory pour apporter d'autres modifications à Active Directory lorsque vous déployez des Blueprints. Reportez-vous à [Utilisation de stratégies Active Directory](#).

Prérequis

- Vérifiez que vous avez au moins une stratégie Active Directory. Reportez-vous à [Créer une stratégie Active Directory](#). Par exemple, vous créez une stratégie de développement qui ajoute des enregistrements à ou=development,dc=corp,dc=domain,dc=com.
- Vérifiez que vous avez un groupe d'activité auquel vous avez appliqué une stratégie Active Directory. Reportez-vous à [Créer un groupe d'activité](#). Par exemple, votre groupe d'activité de développement utilise la stratégie de développement.

Procédure

- 1 Dans votre Blueprint de test, sélectionnez la machine de base de données dans le canevas.
- 2 Cliquez dans l'onglet **Propriétés**.
- 3 Cliquez dans l'onglet **Propriétés personnalisées**.
- 4 Cliquez sur l'icône **Nouveau (+)**.
- 5 Ajoutez la propriété personnalisée pour modifier l'unité d'organisation par défaut.
 - a Dans la zone de texte **Nom**, entrez **ext.policy.activedirectory.orgunit**.
 - b Dans la zone de texte **Valeur**, entrez **ou=databases,dc=corp,dc=domain,dc=com**.
 - c Désélectionnez l'option **Remplaçable**.
 - d Cliquez sur **OK**.
- 6 Cliquez sur **Terminer**.

Le Blueprint de test inclut la propriété personnalisée, mais vos utilisateurs ne la voient pas dans le formulaire de demande.

Suivant

Demandez votre Blueprint de test. Vérifiez que l'enregistrement de la machine de base de données a été ajoutée à l'unité d'organisation de base de données et que l'enregistrement de la machine d'application est ajouté à l'unité d'organisation de développement. Lorsque les résultats vous conviennent, vous pouvez ajouter la propriété personnalisée à vos Blueprints de production.

Fourniture de Blueprints de service aux utilisateurs

3

Vous fournissez des services à la demande aux utilisateurs en créant des éléments de catalogue et des actions, puis en contrôlant avec soin qui peut demander ces services à l'aide de droits d'accès et d'approbations.

Ce chapitre aborde les rubriques suivantes :

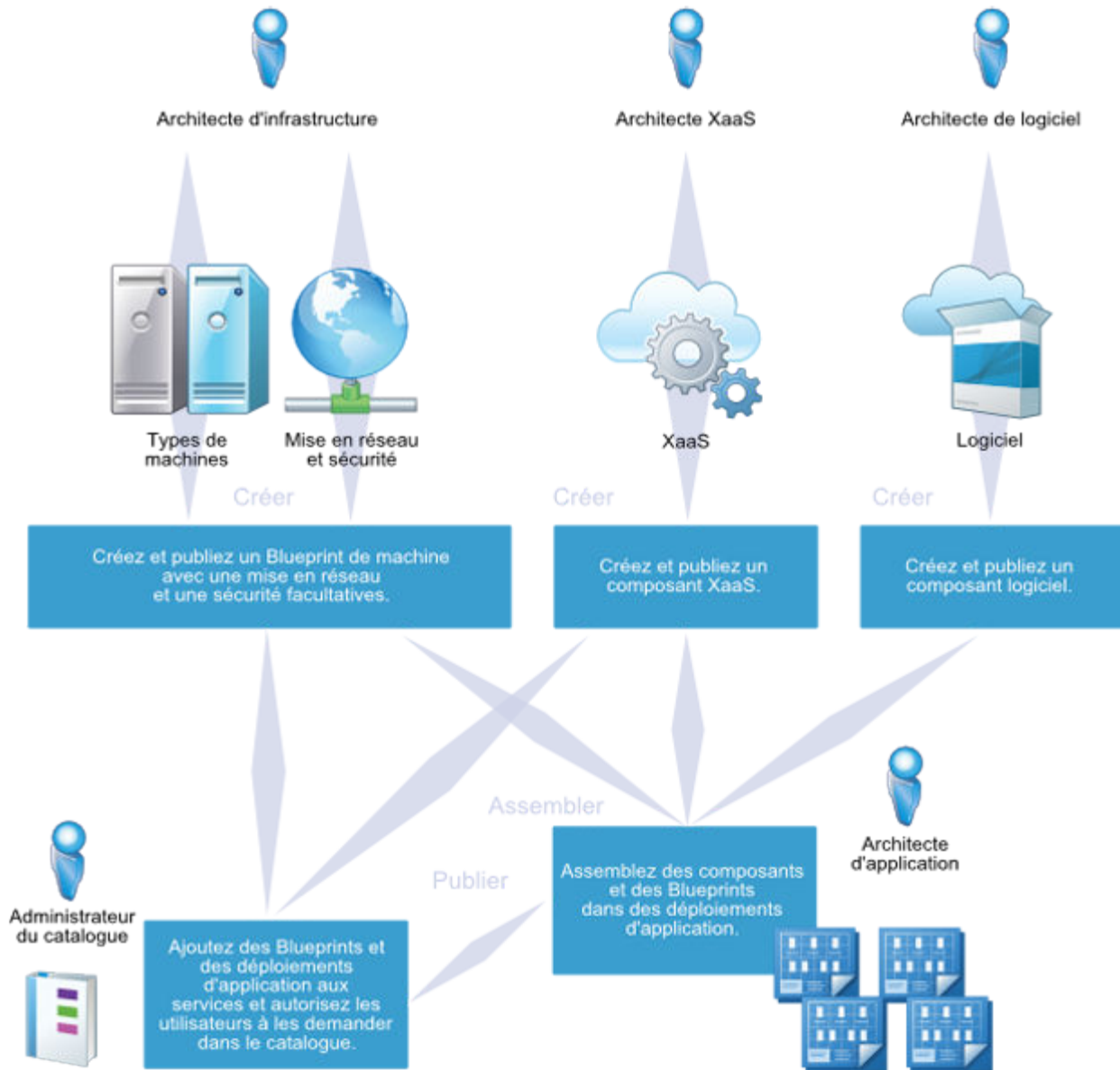
- [Conception de Blueprints](#)
- [Exportation et importation de Blueprints et de contenu](#)
- [Création d'une bibliothèque de conceptions](#)
- [Assemblage de Blueprints composites](#)
- [Gestion du catalogue de services](#)
- [Gestion des éléments de catalogue déployés](#)

Conception de Blueprints

Les architectes de Blueprints construisent les composants Logiciel, les Blueprints de machine et les Blueprints XaaS personnalisés. Ils assemblent ces composants dans les Blueprints qui définissent les éléments demandés par les utilisateurs dans le catalogue.

Vous pouvez créer et publier des Blueprints pour une seule machine ou un Blueprint XaaS unique et personnalisé, mais vous avez aussi la possibilité de combiner des composants de machine et des Blueprints XaaS avec d'autres blocs de construction pour concevoir des Blueprints d'élément de catalogue élaborés qui incluent plusieurs machines, des éléments de réseau et de sécurité, du logiciel avec un support pour toute sa durée de vie et des fonctionnalités XaaS personnalisées.

Selon l'élément de catalogue que vous souhaitez définir, la procédure peut être aussi simple qu'un architecte d'infrastructure unique publiant un composant de machine sous forme de Blueprint ou alors inclure plusieurs architectes créant de nombreux types de composants pour concevoir une pile d'application complète à laquelle les utilisateurs peuvent faire appel.



Les composants de Logiciel

Vous pouvez créer et publier des composants logiciels à installer lors du provisionnement de la machine permettant de prendre en charge le cycle de vie du logiciel. Par exemple, vous pouvez créer un Blueprint permettant aux développeurs de faire appel à une machine avec leur environnement de développement déjà installé et configuré. Les composants logiciels ne sont pas des éléments de catalogue en soi. Vous devez les combiner à un composant de machine pour créer un Blueprint d'élément de catalogue.

Blueprints de machines

Vous pouvez créer et publier des Blueprints simples pour provisionner les machines ou créer plusieurs Blueprints complexes contenant des composants de machine supplémentaires, qui peuvent également contenir n'importe quelle combinaison des types de composants suivants :

- Composants Logiciel
- Blueprints existants
- Composants réseau et de sécurité NSX
- Composants XaaS
- Composants Conteneurs
- Composants personnalisés ou autres

Blueprints XaaS

Vous pouvez publier vos workflows vRealize Orchestrator en tant que Blueprints XaaS. Par exemple, vous pouvez créer une ressource personnalisée pour les utilisateurs Active Directory et concevoir un Blueprint XaaS pour permettre aux gestionnaires de provisionner de nouveaux utilisateurs dans leur groupe Active Directory. Vous créez et gérez des composants XaaS hors de l'onglet de conception. Vous pouvez réutiliser des Blueprints XaaS publiés pour créer des Blueprints d'application, mais uniquement en combinaison avec au moins un composant de machine.

Blueprints d'application avec plusieurs machines, XaaS et composants Logiciel

Vous pouvez ajouter le nombre désiré de composants de machine, de composants Logiciel et de Blueprints XaaS à un Blueprint de machine pour fournir des fonctionnalités à vos utilisateurs.

Par exemple, vous pouvez créer un Blueprint pour les gestionnaires, afin qu'ils provisionnent une configuration de nouvelle embauche. Vous pouvez combiner plusieurs composants de machine, composants logiciels et un Blueprint XaaS pour le provisionnement de nouveaux utilisateurs Active Directory. Le gestionnaire QE peut faire appel à votre élément de catalogue de nouvelle embauche et ses nouveaux ingénieurs qualité sont provisionnés dans Active Directory et reçoivent deux machines virtuelles, une exécutant Windows, l'autre Linux, avec tous les logiciels nécessaires pour réaliser des tests dans ces environnements.

Exportation et importation de Blueprints et de contenu

Vous pouvez exporter des Blueprints et du contenu par programme d'un environnement vRealize Automation à un autre au moyen de l'API REST vRealize Automation ou de vRealize CloudClient.

Par exemple, vous pouvez créer et tester vos Blueprints dans un environnement de développement, puis les importer dans votre environnement de production. Vous pouvez également importer une définition de propriété d'un forum communautaire dans l'instance de votre locataire vRealize Automation actif.

Vous pouvez importer et exporter par programme n'importe quel contenu vRealize Automation suivant :

- Blueprints d'application et tous leurs composants
- Blueprints de machines IaaS
- Les composants de Logiciel
- Blueprints XaaS
- Profils de composants
- Groupes de propriétés

Les informations d'un groupe de propriétés sont spécifiques à un locataire et sont uniquement importés avec le Blueprint si le groupe de propriétés existe déjà dans l'instance cible de vRealize Automation.

Lorsque vous exportez un Blueprint à partir d'une instance de vRealize Automation dans un autre, les informations du groupe de propriétés définies pour ce Blueprint ne sont pas reconnues pour le Blueprint importé sauf si le groupe de propriétés existe déjà dans l'instance du locataire cible. Par exemple, si vous importez un Blueprint qui contient un groupe de propriétés nommé `mica1`, le groupe de propriétés `mica1` n'est pas présent dans le Blueprint importé sauf si le groupe importé `mica1` existe déjà dans l'instance de vRealize Automation où vous importez le Blueprint. Pour éviter de perdre des informations sur un groupe de propriétés lors de l'exportation d'un Blueprint d'une instance de vRealize Automation vers une autre, utilisez vRealize CloudClient pour créer un fichier zip de module d'exportation qui contient le groupe de propriétés et importez ce fichier zip de module dans le locataire cible avant d'importer le Blueprint. Pour plus d'informations sur l'utilisation de vRealize CloudClient pour répertorier, conditionner, exporter et importer des groupes de propriétés, ainsi que d'autres éléments vRealize Automation, reportez-vous au Centre des développeurs VMware à l'adresse <https://developercenter.vmware.com/tool/cloudclient>.

Tableau 3-1. Sélection de votre outil d'importation et d'exportation

Outil	Plus d'informations
vRealize CloudClient	Reportez-vous au centre des développeurs VMware à l'adresse https://developercenter.vmware.com/tool/cloudclient .
API REST vRealize Automation	Reportez-vous au <i>Guide de programmation</i> dans le centre d'informations de vRealize Automation à l'adresse https://www.vmware.com/support/pubs/vcac-pubs.html .

Remarque Lors de l'exportation et de l'importation de Blueprints par programmation dans les déploiements de vRealize Automation, par exemple depuis un test vers un environnement de production ou depuis une organisation à une autre, il est important de reconnaître que les données du modèle de clone sont incluses dans le module. Lorsque vous importez le module de Blueprints, les paramètres par défaut sont renseignés en fonction des informations contenues dans le package. Par exemple, si vous exportez, puis importez un Blueprint qui a été créé à l'aide d'un workflow de style de clone et que le modèle dont les données clonées ont été dérivées n'existe pas dans un point de terminaison du déploiement de vRealize Automation dans lequel vous importez le Blueprint, certains paramètres importés du Blueprint ne sont pas applicables à ce déploiement.

Scénario : Importer l'exemple d'application Dukes Bank pour vSphere et le configurer pour votre environnement

En tant que professionnel de l'informatique en cours d'évaluation ou d'apprentissage de vRealize Automation, vous souhaitez importer un échantillon d'application stable dans votre instance de vRealize Automation afin d'explorer rapidement la fonctionnalité disponible et de déterminer comment créer des Blueprints de vRealize Automation répondant aux besoins de votre organisation.

Prérequis

- Préparez une machine de référence Linux CentOS 6.x, convertissez-la en un modèle et créez une spécification de personnalisation. Reportez-vous à [Scénario : Préparer l'importation du Blueprint de l'exemple d'application Dukes Bank pour vSphere](#).
- Créez un profil réseau externe pour fournir une passerelle et une plage d'adresses IP. Reportez-vous à [Créer un profil de réseau externe au moyen d'un fournisseur IPAM tiers](#).
- Mappez votre profil réseau externe à votre réservation vSphere. Reportez-vous à [Créer une réservation pour Hyper-V, KVM, SCVMM, vSphere ou XenServer](#). L'exemple d'application ne peut pas être provisionné correctement sans un profil réseau externe.
- Vérifiez que vous disposez des privilèges d'**architecte d'infrastructure** et d'**architecte de logiciel**. Les deux rôles sont requis pour importer l'exemple d'application Dukes Bank et pour interagir avec les Blueprints et les composants logiciels Dukes Bank.

Procédure

1 Scénario : Importer l'exemple d'application Dukes Bank pour vSphere

Vous téléchargez l'application Dukes Bank pour vSphere à partir de votre dispositif vRealize Automation. Vous importez l'exemple d'application dans votre locataire vRealize Automation pour afficher un exemple de travail d'un Blueprint vRealize Automation multiniveau qui inclut plusieurs composants de machine avec des composants logiciels et de mise en réseau.

2 Scénario : Configurer des exemples de composants vSphere Dukes Bank pour votre environnement

À l'aide de vos privilèges d'architecte d'infrastructure, vous configurez chacun des composants de machine Dukes Bank pour utiliser les préfixes de spécification de personnalisation, modèle et machine que vous avez créés pour votre environnement.

Vous avez configuré Dukes Bank pour l'exemple d'application vSphere pour votre environnement afin de l'utiliser comme point de départ pour le développement de vos propres Blueprints, en tant qu'outil d'évaluation de vRealize Automation ou comme ressource d'apprentissage vous permettant de comprendre la fonctionnalité et les composants vRealize Automation.

Scénario : Importer l'exemple d'application Dukes Bank pour vSphere

Vous téléchargez l'application Dukes Bank pour vSphere à partir de votre dispositif vRealize Automation. Vous importez l'exemple d'application dans votre locataire vRealize Automation pour afficher un exemple de travail d'un Blueprint vRealize Automation multiniveau qui inclut plusieurs composants de machine avec des composants logiciels et de mise en réseau.

Procédure

- 1 Connectez-vous au dispositif vRealize Automation en tant qu'utilisateur racine à l'aide du protocole SSH.
- 2 Téléchargez l'exemple d'application Dukes Bank pour vSphere à partir de votre dispositif vRealize Automation dans /tmp.

```
wget --no-check-certificate https://vRealize_VA_Hostname_fqdn:5480/blueprints/DukesBankAppForvSphere.zip
```

Ne décompressez pas le module.

- 3 Téléchargez vRealize CloudClient de <http://developercenter.vmware.com/tool/cloudclient> dans /tmp.
- 4 Décompressez le module cloudclient-4x-dist.zip.
- 5 Exécutez vRealize CloudClient dans le répertoire /bin.

```
$>./bin/cloudclient.sh
```

- 6 Si vous y êtes invité, acceptez le contrat de licence.

- 7 À l'aide de vRealize CloudClient, connectez-vous au dispositif vRealize Automation en tant qu'utilisateur disposant de privilèges d'**architecte de logiciel** et d'**architecte d'infrastructure**.

```
CloudClient>vra login userpass --server https://vRealize_VA_Hostname_fqdn --user <user@domain.com>
--tenant <TenantName>
```

- 8 Lorsque vous y êtes invité, entrez le mot de passe de connexion.
- 9 Confirmez la disponibilité du contenu du fichier DukesBankAppForvSphere.zip.

```
vra content import --path /<Chemin>/DukesBankAppForvSphere.zip --dry-run true --resolution
OVERWRITE
```

Notez que l'entrée REMPLACER est sensible à la casse et requiert des majuscules.

En configurant la résolution à remplacer plutôt que *skip*, vous autorisez vRealize Automation à corriger les conflits lorsque cela est possible.

- 10 Importez l'exemple d'application Dukes Bank.

```
vra content import --path /<Chemin>/DukesBankAppForvSphere.zip --dry-run false --resolution
OVERWRITE
```

Notez que l'entrée REMPLACER est sensible à la casse et requiert des majuscules.

Lorsque vous vous connectez à la console vRealize Automation en tant qu'utilisateur disposant de privilèges d'architecte de logiciel et d'architecte d'infrastructure, vous voyez les Blueprints et les composants logiciels Dukes Bank dans l'onglet **Conception > Blueprints** et l'onglet **Conception > Composants logiciels**.

Scénario : Configurer des exemples de composants vSphere Dukes Bank pour votre environnement

À l'aide de vos privilèges d'architecte d'infrastructure, vous configurez chacun des composants de machine Dukes Bank pour utiliser les préfixes de spécification de personnalisation, modèle et machine que vous avez créés pour votre environnement.

Ce scénario configure les composants de machine pour cloner des machines à partir du modèle que vous avez créé dans le client Web vSphere. Si vous souhaitez créer des copies d'une machine virtuelle à optimisation d'espace sur un snapshot, l'échantillon d'application prend également en charge les clones liés. Les clones liés utilisent une chaîne de disques delta pour effectuer le suivi des différences avec une machine parent, sont provisionnés rapidement, réduisent le coût de stockage et sont parfaits à utiliser lorsque les performances ne sont pas prioritaires.

Procédure

- 1 Connectez-vous à la console vRealize Automation en tant qu'**architecte d'infrastructure**.

Vous pouvez configurer l'exemple d'application Dukes Bank pour fonctionner dans votre environnement uniquement avec le rôle d'**architecte d'infrastructure**, mais si vous souhaitez afficher ou modifier les composants logiciels du modèle, vous avez également besoin du rôle d'**architecte de logiciels**.

- 2 Sélectionnez **Conception > Blueprints**.

- 3 Sélectionnez le Blueprint **DukesBankApplication** et cliquez sur l'icône **Modifier**.

- 4 Modifiez le composant appserver-node afin que vRealize Automation puisse provisionner ce composant de machine dans votre environnement.

Vous configurez le Blueprint pour provisionner plusieurs instances de ce composant de machine de sorte que vous puissiez vérifier la fonctionnalité du nœud d'équilibrage de charge.

- a Cliquez sur le composant **appserver-node** sur le canevas de conception.

Les détails de la configuration s'affichent dans le volet du bas.

- b Sélectionnez votre préfixe de machine dans le menu déroulant **Préfixe de machine**.

- c Configurez votre Blueprint pour provisionner de deux instances à dix instances de ce nœud en sélectionnant 2 instances au minimum et 10 instances au maximum.

Sur le formulaire de demande, les utilisateurs peuvent provisionner de deux à dix nœuds appserver. S'ils sont autorisés à exécuter des actions de réduction de charge ou de montée en charge, les utilisateurs peuvent dimensionner leur déploiement pour répondre à l'évolution des besoins.

- d Cliquez sur l'onglet **Informations sur le build**.

- e Sélectionnez **Cloner le workflow** dans le menu déroulant **Workflow de provisionnement**.

- f Sélectionnez votre modèle **dukes_bank_template** dans la boîte de dialogue **Cloner à partir de**.

- g Entrez votre modèle **Customspecs_sample** dans la zone de texte **Spécification de personnalisation**.

Ce champ est sensible à la casse.

- h Cliquez sur l'onglet **Ressources de machine**.

- i Vérifiez que la machine dispose d'au moins 2 048 Mo de mémoire.

- 5 Modifiez le nœud d'équilibrage de charge afin que vRealize Automation puisse provisionner ce composant de machine dans votre environnement.

- a Cliquez sur le composant **loadbalancer-node** sur le canevas de conception.///

- b Sélectionnez votre préfixe de machine dans le menu déroulant **Préfixe de machine**.

- c Cliquez sur l'onglet **Informations sur le build**.

- d Sélectionnez **Cloner le workflow** dans le menu déroulant **Workflow de provisionnement**.

- e Sélectionnez votre modèle **dukes_bank_template** dans la boîte de dialogue **Cloner à partir de**.
 - f Entrez votre modèle **Customspecs_sample** dans la zone de texte **Spécification de personnalisation**.
Ce champ est sensible à la casse.
 - g Cliquez sur l'onglet **Ressources de machine**.
 - h Vérifiez que la machine dispose d'au moins 2 048 Mo de mémoire.
- 6** Répétez ces étapes pour le composant de machine **database-node**.
- 7** Cliquez sur **Enregistrer et terminer**.
Vos modifications sont enregistrées et vous revenez à l'onglet **Blueprints**.
- 8** Sélectionnez le Blueprint **DukesBankApplication** et cliquez sur **Publier**.

Vous avez configuré l'échantillon de Blueprint d'application Dukes Bank pour votre environnement et publié le Blueprint terminé.

Suivant

Les Blueprints publiés ne s'affichent pas dans le catalogue pour les utilisateurs tant que vous n'avez pas configuré un service de catalogue, ajouté le Blueprint à un service, ni autorisé les utilisateurs à demander votre Blueprint. Reportez-vous à [Liste de contrôle pour la configuration du catalogue de services](#).

Après avoir configuré votre Blueprint Dukes Bank pour qu'il s'affiche dans le catalogue, vous pouvez demander à provisionner l'échantillon de l'application. Reportez-vous à [Scénario : test de l'exemple d'application Dukes Bank](#).

Scénario : test de l'exemple d'application Dukes Bank

Faites appel à l'élément de catalogue Dukes Bank et connectez-vous à l'exemple d'application pour vérifier votre travail et afficher la fonctionnalité Blueprint vRealize Automation.

Prérequis

- Importez l'exemple d'application Dukes Bank et configurez les composants de Blueprint pour travailler dans votre environnement. Reportez-vous à [Scénario : Importer l'exemple d'application Dukes Bank pour vSphere et le configurer pour votre environnement](#).
- Configurez le catalogue de services et rendez votre Blueprint Dukes Bank publié disponible pour que les utilisateurs puissent le demander. Reportez-vous à [Liste de contrôle pour la configuration du catalogue de services](#).
- Vérifiez que les machines virtuelles que vous provisionnez peuvent atteindre le référentiel YUM.

Procédure

- 1 Connectez-vous à la console vRealize Automation en tant qu'utilisateur avec droit d'accès à l'élément de catalogue Dukes Bank.
- 2 Cliquez sur l'onglet **Catalogue**.

- 3 Localisez l'élément de catalogue de l'exemple d'application Dukes Bank et cliquez sur **Demande**.
- 4 Fournissez les informations de demande requises pour chaque composant accompagné d'une astérisque rouge.
 - a Accédez au composant JBossAppServer pour remplir les informations de demande requises.
 - b Entrez le nom de domaine complet de votre dispositif vRealize Automation dans la zone de texte **app_content_server_ip**.
 - c Accédez aux composants logiciels Dukes_Bank_App pour remplir les informations de demande requises.
 - d Entrez le nom de domaine complet de votre dispositif vRealize Automation dans les zones de texte **app_content_server_ip**.
- 5 Cliquez sur **Envoyer**.

Selon votre réseau et votre instance vCenter Server, 15 à 20 minutes peuvent être nécessaires pour provisionner intégralement l'exemple d'application Dukes Bank. Vous pouvez surveiller l'état dans l'onglet **Demandes** et, une fois l'application provisionnée, vous pouvez afficher les détails de l'élément de catalogue dans l'onglet **Éléments**.
- 6 Une fois l'application provisionnée, localisez l'adresse IP du serveur de l'équilibrage de charge afin d'accéder à l'exemple d'application Dukes Bank.
 - a Sélectionnez **Éléments > Déploiements**.
 - b Développez votre déploiement d'exemple d'application Dukes Bank et sélectionnez le serveur de l'équilibrage de charge Apache.
 - c Cliquez sur **Afficher les détails**.
 - d Sélectionnez l'onglet **Réseau**.
 - e Notez l'adresse IP.
- 7 Connectez-vous à l'exemple d'application Dukes Bank.
 - a Accédez au serveur de l'équilibrage de charge à l'adresse `http://IP_Apache_Load_Balancer:8081/bank/main.faces`.

Si vous voulez accéder directement aux serveurs d'application, vous pouvez vous rendre à l'adresse `http://IP_AppServer:8080/bank/main.faces`.
 - b Entrez **200** dans la zone de texte **Nom d'utilisateur**.
 - c Entrez **foobar** dans la zone de texte **Mot de passe**.

Vous avez un échantillon d'application Dukes Bank fonctionnel à utiliser comme point de départ pour le développement de vos propres Blueprints, en tant qu'outil d'évaluation de vRealize Automation ou comme ressource d'apprentissage vous permettant de comprendre la fonctionnalité et les composants vRealize Automation.

Création d'une bibliothèque de conceptions

Vous pouvez créer une bibliothèque de composants de Blueprint réutilisables que les architectes peuvent assembler en Blueprints d'application afin d'offrir aux utilisateurs des services à la demande élaborés.

Créez une bibliothèque des plus petits composants de conception du Blueprint : Blueprints de machine unique, composants Logiciel et Blueprints XaaS. Ensuite, combinez ces blocs constitutifs de base de façon inédite afin de créer des éléments de catalogue élaborés qui fournissent un niveau croissant de fonctionnalité aux utilisateurs.

Notez que les exemples de Blueprints sont disponibles sur la page VMware Solution Exchange à l'adresse <https://solutionexchange.vmware.com> et à l'adresse <https://code.vmware.com>.

Tableau 3-2. Création d'une bibliothèque de conceptions

Élément du catalogue	Rôle	Composants	Description	Détails
Machines	Architecte d'infrastructure	Créez des Blueprints de machine dans l'onglet Blueprints .	<p>Vous pouvez créer des Blueprints de machine pour rapidement livrer à vos utilisateurs des machines virtuelles, privées et publiques, ou des machines de cloud hybride.</p> <p>Les administrateurs du catalogue disposent de Blueprints de machine publiés à inclure dans le catalogue en tant que Blueprints autonomes, mais vous pouvez également combiner des Blueprints de machines avec d'autres composants pour créer des éléments de catalogue plus élaborés qui incluent plusieurs Blueprints de machine Logiciel ou des Blueprints XaaS.</p>	Configurer un Blueprint de machine
Réseau et sécurité NSX sur les machines	Architecte d'infrastructure	Ajoutez des composants de réseau et de sécurité NSX à des Blueprints de machine vSphere dans l'onglet Blueprints .	<p>Vous pouvez configurer des composants de réseau et de sécurité tels que des profils réseau et des groupes de sécurité, pour permettre aux machines virtuelles de communiquer entre elles sur des réseaux physiques et virtuels efficacement et en toute sécurité.</p> <p>Vous devez combiner des composants de réseau et de sécurité avec au moins un composant de machine vSphere avant que les administrateurs du catalogue puissent les inclure dans le catalogue. Vous ne pouvez appliquer des composants de réseau et de sécurité NSX qu'à des Blueprints de machine vSphere.</p>	Conception de Blueprints avec des paramètres NSX

Tableau 3-2. Création d'une bibliothèque de conceptions (suite)

Élément du catalogue	Rôle	Composants	Description	Détails
Logiciel sur les machines	<p>Architecte de logiciel</p> <p>Pour ajouter des composants logiciels avec succès au canevas de conception, vous devez également disposer des rôles de membre du groupe d'activité, d'administrateur de groupe d'activité ou d'administrateur de locataire afin d'accéder au catalogue cible.</p>	<p>Créez et publiez des composants Logiciel dans l'onglet Logiciel, puis combinez-les avec des Blueprints de machine dans l'onglet Blueprints.</p>	<p>Ajoutez les composants Logiciel à vos Blueprints de machine pour normaliser, déployer, configurer, mettre à jour et dimensionner des applications complexes dans des environnements de cloud. Ces applications peuvent varier de la simple application Web à une application personnalisée très élaborée et modularisée.</p> <p>Les composants Logiciel ne peuvent pas figurer seuls dans le catalogue. Vous devez créer et publier les composants Logiciel, puis assembler un Blueprint d'application qui contient au moins une machine.</p>	<p>Créer un composant Logiciel</p>

Tableau 3-2. Création d'une bibliothèque de conceptions (suite)

Élément du catalogue	Rôle	Composants	Description	Détails
Services informatiques personnalisés	Architectes XaaS	Créez et publiez des Blueprints XaaS dans l'onglet XaaS .	<p>Vous pouvez créer des éléments de catalogue XaaS qui étendent la fonctionnalité vRealize Automation au-delà du provisionnement de machine, de mise en réseau, de sécurité et de logiciel. À l'aide de workflows et de plug-ins vRealize Orchestrator existants, ou de scripts personnalisés développés dans vRealize Orchestrator, vous pouvez automatiser la livraison de n'importe quel service informatique.</p> <p>Les administrateurs du catalogue disposent de Blueprints XaaS publiés à inclure dans le catalogue en tant que Blueprints autonomes, mais vous pouvez également les combiner avec d'autres composants dans l'onglet Blueprints pour créer des éléments de catalogue plus élaborés.</p>	Conception de Blueprints XaaS et d'actions sur les ressources
Assembler les composants de base des Blueprints publiés en nouveaux éléments de catalogue	<ul style="list-style-type: none"> ■ Architecte d'application ■ Architecte d'infrastructure ■ Architecte de logiciel 	<p>Combinez des Blueprints de machine supplémentaires, des Blueprints XaaS et des composants Logiciel avec au moins un composant ou un Blueprint de machine dans l'onglet Blueprints.</p>	<p>Vous pouvez réutiliser des composants et des Blueprints publiés en les combinant d'une nouvelle façon afin de créer des modules de services informatiques qui offrent une fonctionnalité élaborée aux utilisateurs.</p>	Assemblage de Blueprints composites

Conception de Blueprints de machine

Les Blueprints de machine sont la spécification complète d'une machine, déterminant les attributs de la machine, la manière dont elle est provisionnée et ses paramètres de stratégie et de gestion. En fonction de la complexité de l'élément de catalogue que vous créez, vous pouvez associer un ou plusieurs composants de machine dans un Blueprint à d'autres composants dans le canevas de conception pour créer des éléments de catalogue plus élaborés qui incluent la mise en réseau et la sécurité, les composants Logiciel, les composants XaaS et les autres composants du Blueprint.

Stockage à optimisation d'espace pour le provisionnement virtuel

La technologie de stockage à optimisation d'espace élimine les inefficacités des méthodes de stockage traditionnelles en utilisant uniquement le stockage réellement requis pour les opérations d'une machine. En général, il s'agit uniquement d'une fraction du stockage réellement alloué aux machines. vRealize Automation prend en charge deux méthodes de provisionnement avec la technologie d'optimisation de l'espace, le provisionnement dynamique et le provisionnement FlexClone.

Lorsque le stockage standard est utilisé, le stockage alloué à une machine provisionnée est entièrement dédié à cette machine, même quand elle est hors tension. Cela peut constituer un gaspillage important des ressources de stockage, car peu de machines virtuelles utilisent réellement l'ensemble du stockage qui leur est alloué. Seules quelques machines physiques fonctionnent avec un disque plein à 100 %. Quand une technologie de stockage à optimisation d'espace est utilisée, le suivi du stockage alloué et du stockage utilisé est effectué séparément et seul le stockage utilisé est entièrement dédié à la machine provisionnée.

Thin Provisioning

Le provisionnement dynamique est pris en charge pour toutes les méthodes de provisionnement virtuel. En fonction de votre plate-forme de virtualisation, de votre type de stockage et de la configuration de stockage par défaut, le provisionnement dynamique peut toujours être utilisé pendant le provisionnement de la machine. Par exemple, le provisionnement dynamique est toujours utilisé pour les intégrations de vSphere ESX Server qui font appel au stockage NFS. En revanche, pour les intégrations vSphere ESX Server utilisant du stockage local ou iSCSI, le provisionnement dynamique est uniquement utilisé pour provisionner des machines si la propriété `VirtualMachine.Admin.ThinProvision` est spécifiée dans le Blueprint. Pour plus d'informations sur le provisionnement dynamique, reportez-vous à la documentation fournie par votre plate-forme de virtualisation.

Provisionnement Net App FlexClone

Vous pouvez créer un Blueprint pour le provisionnement Net App FlexClone si vous travaillez dans un environnement vSphere qui utilise le stockage Network File System (NFS) et la technologie FlexClone.

Vous ne pouvez utiliser que le stockage NFS, sinon le provisionnement de la machine échoue. Vous pouvez spécifier un chemin de stockage FlexClone pour d'autres types de provisionnement de machine, mais le chemin de stockage FlexClone agit comme le stockage standard.

Voici une présentation générale de la procédure requise pour provisionner des machines qui reposent sur la technologie FlexClone :

- 1 Un administrateur IaaS crée un point de terminaison NetApp ONTAP. Reportez-vous à [Référence des paramètres de point de terminaison](#).
- 2 Un administrateur IaaS exécute une collecte de données sur le point de terminaison pour rendre celui-ci visible sur les pages de ressource de calcul et de réservation.

L'option FlexClone est visible sur la page de réservation dans la colonne des points de terminaison s'il existe un point de terminaison NetApp ONTAP et si l'hôte est virtuel. S'il existe un point de terminaison NetApp ONTAP, la page de réservation affiche le point de terminaison attribué au chemin de stockage.

- 3 Un administrateur Fabric crée une réservation vSphere, active le stockage FlexClone et spécifie un chemin de stockage NFS qui s'appuie sur la technologie FlexClone. Reportez-vous à [Créer une réservation pour Hyper-V, KVM, SCVMM, vSphere ou XenServer](#).
- 4 Un architecte d'infrastructure ou un autre utilisateur autorisé crée un Blueprint pour le provisionnement FlexClone.

Présentation et utilisation du paramétrage de Blueprint

Vous pouvez utiliser des profils de composants pour paramétrer les Blueprints. Plutôt que de créer un Blueprint de petite, moyenne et grande taille distinct pour un type de déploiement spécifique, vous pouvez créer un Blueprint unique avec un choix de machine virtuelle de petite, moyenne ou grande taille. Les utilisateurs peuvent sélectionner l'une de ces tailles lorsqu'ils déploient l'élément du catalogue.

Les profils de composants réduisent la prolifération de Blueprints et simplifient vos offres du catalogue. Vous pouvez utiliser les profils de composants pour définir les composants de machine vSphere dans un Blueprint. Les types de profils de composants disponibles sont Size et Image. Lorsque vous ajoutez des profils de composants à un composant de machine, les paramètres du profil du composant remplacent les paramètres du composant de machine, notamment le nombre de CPU ou le volume de stockage.

Les profils de composants sont uniquement disponibles pour les composants de machine vSphere.

Pour plus d'informations sur la définition d'ensembles de valeurs pour les profils de composants Size et Image, reportez-vous à la section dans *Référence des propriétés personnalisées*

Pour plus d'informations sur l'ajout des profils de composants et des ensembles de valeurs sélectionnés pour un composant de machine vSphere dans un Blueprint, reportez-vous à la section [Paramètres du composant de machine vSphere](#).

Pour plus d'informations sur l'utilisation des profils de composants lors de la demande de provisionnement d'une machine, reportez-vous à la section [Demander le provisionnement de machine à l'aide d'un Blueprint paramétré](#).

Remarque Vous pouvez créer des stratégies d'approbation pour exiger une approbation préalable lors de la demande de provisionnement machine de Blueprints par rapport aux conditions d'ensemble de valeurs des profils de composants Size et Image. Pour plus d'informations, reportez-vous à la section [Exemples de stratégies d'approbation basées sur le type de stratégie de machine virtuelle](#).

Pour plus d'informations sur l'utilisation du paramétrage du Blueprint lors de la demande de provisionnement machine à partir du catalogue, reportez-vous à la section [Demander le provisionnement de machine à l'aide d'un Blueprint paramétré](#).

Configurer un Blueprint de machine

Configurer et publier un composant de la machine en tant que Blueprint autonome que d'autres architectes peuvent réutiliser en tant que composant dans les Blueprints d'application et que les administrateurs du catalogue peuvent inclure dans les services du catalogue.

Prérequis

- Connectez-vous à la console vRealize Automation en tant qu'**architecte d'infrastructure**.
- Terminez les préparations externes pour le provisionnement, comme la création de modèles, WinPE et ISO, ou regroupez les informations sur les préparations externes provenant de vos administrateurs.
- Configurez le locataire. Reportez-vous à [Configuration des paramètres de locataire](#).
- Configurez les ressources IaaS. Reportez-vous à [Liste de contrôle pour la configuration de ressources IaaS](#).
- Reportez-vous à *Configuration de vRealize Automation*.

Procédure

- 1 Sélectionnez **Conception > Blueprints**.
- 2 Cliquez sur l'icône **Nouveau (+)**.
- 3 Pour configurer les paramètres généraux, suivez les invites de la boîte de dialogue **Nouveau Blueprint**.

- 4 Cliquez sur **OK**.
- 5 Cliquez sur **Types de machines** dans la zone Catégories pour afficher la liste des types de machines disponibles.
- 6 Faites glisser le type de machine que vous souhaitez provisionner vers le canevas de conception.
- 7 Suivez les invites sur chacun des onglets pour configurer les détails du provisionnement de la machine.
- 8 Cliquez sur **Terminer**.
- 9 Sélectionnez votre Blueprint et cliquez sur **Publier**.

Vous avez configuré et publié un composant de la machine en tant que Blueprint autonome. Les administrateurs du catalogue peuvent inclure ce Blueprint de machine dans les services du catalogue et autoriser les utilisateurs à demander ce Blueprint. D'autres architectes peuvent réutiliser ce Blueprint de machine afin de créer des Blueprints d'application plus élaborés comprenant des composants Logiciel, des Blueprints XaaS ou des Blueprints de machine supplémentaires.

Suivant

Vous pouvez combiner un Blueprint de machine avec des composants Logiciel, des Blueprints XaaS ou des Blueprints de machine supplémentaires pour créer des Blueprints d'application élaborés. Reportez-vous à [Assemblage de Blueprints composites](#).

Paramètres de Blueprint de machine

Vous pouvez définir des paramètres de configuration et des propriétés personnalisées pour le Blueprint global.

Paramètres des propriétés de Blueprint

Vous pouvez spécifier des paramètres qui s'appliquent à l'intégralité du Blueprint à l'aide de la page **Nouveau Blueprint** lorsque vous créez le Blueprint. Après avoir créé le Blueprint, vous pouvez modifier ces paramètres dans la boîte de dialogue Propriétés du Blueprint.

Onglet Général

Appliquez des paramètres à votre Blueprint entier, y compris tous les composants que vous envisagez d'ajouter maintenant ou ultérieurement.

Tableau 3-3. Paramètres de l'onglet Général

Configuration	Description
Nom	Entrez le nom de votre Blueprint.
Identifiant	Le champ Identifiant est automatiquement renseigné avec le nom que vous avez entré. Vous pouvez modifier ce champ maintenant, mais une fois le Blueprint enregistré, vous ne pourrez plus le modifier. Du fait que les identifiants sont permanents et uniques au sein de votre locataire, vous pouvez les utiliser pour interagir par programmation avec les Blueprints et pour créer des liaisons de propriétés.

Tableau 3-3. Paramètres de l'onglet Général (suite)

Configuration	Description
Description	Résumez votre Blueprint à l'attention d'autres architectes. Cette description apparaît également aux utilisateurs spécifiés sur le formulaire de demande.
Archiver (jours)	Vous pouvez spécifier une période d'archivage pour conserver les déploiements de manière temporaire plutôt que détruire les déploiements dès l'expiration de leur bail. Spécifiez 0 (par défaut) pour détruire le déploiement à l'expiration de son bail. La période d'archivage commence le jour d'expiration du bail. À l'expiration de la période d'archivage, le déploiement est détruit.
Limite de déploiement	Spécifiez le nombre maximal de déploiements qui peuvent être créés lorsque ce Blueprint est utilisé pour provisionner des machines.
Bail (jours) : minimum et maximum	Entrez une valeur minimale et une valeur maximale pour permettre aux utilisateurs de choisir parmi plusieurs durées de bail. Lorsque le bail se termine, le déploiement est détruit ou archivé. Si vous ne spécifiez pas de valeurs minimale et maximale, le bail devient perpétuel.

Onglet Paramètres NSX

Si vous avez configuré NSX, vous pouvez spécifier la zone de transport NSX, la stratégie de réservation de passerelle Edge et acheminée, et les paramètres d'isolation d'application lorsque vous créez ou modifiez un Blueprint. Ces paramètres sont disponibles dans l'onglet **Paramètres NSX** sur les pages **Blueprint** et **Propriétés du Blueprint**.

Pour plus d'informations sur les paramètres de NSX, reportez-vous à [Paramètres de la page Nouveau Blueprint et Propriétés du Blueprint avec NSX](#).

Onglet Propriétés

Les propriétés personnalisées que vous ajoutez au niveau du Blueprint s'appliquent à l'intégralité du Blueprint, y compris l'ensemble de ses composants. Cependant, elles peuvent être remplacées par des propriétés personnalisées attribuées ultérieurement dans la chaîne de priorité. Pour plus d'informations sur l'ordre de priorité des propriétés personnalisées, reportez-vous à *Référence des propriétés personnalisées*.

Tableau 3-4. Paramètres de l'onglet **Propriétés**

Onglet	Configuration	Description
Groupes de propriétés		Les groupes de propriétés sont des groupes de propriétés réutilisables qui sont destinés à simplifier le processus d'ajout de propriétés personnalisées aux Blueprints. Vos gestionnaires de locataires et administrateurs Fabric peuvent regrouper les propriétés qui sont souvent utilisées ensemble de sorte que vous puissiez ajouter le groupe de propriétés à un Blueprint plutôt qu'insérer individuellement des propriétés personnalisées.
	Ajouter	<p>Ajoutez un ou plusieurs groupes de propriétés existants et appliquez-les au Blueprint global.</p> <p>Les groupes de propriétés liées à des conteneurs suivants sont fournis :</p> <ul style="list-style-type: none"> ■ Propriétés de l'hôte du conteneur avec authentification par certificat ■ Propriétés de l'hôte du conteneur avec authentification par utilisateur/mot de passe
	Monter /Descendre	Contrôlez l'ordre de priorité donné à chaque groupe de propriétés par rapport aux autres en classant les groupes par ordre de priorité. Le premier groupe de la liste a le niveau de priorité le plus élevé et ses propriétés personnalisées sont prioritaires. Vous pouvez également utiliser la fonction de glisser-déposer pour changer l'ordre.
	Afficher les propriétés	Affichez les propriétés personnalisées du groupe de propriétés sélectionné.
	Afficher les propriétés fusionnées	Si une propriété personnalisée est incluse dans plusieurs groupes de propriétés, la valeur incluse dans le groupe de propriétés avec le niveau de priorité le plus élevé est prioritaire. Vous pouvez afficher ces propriétés fusionnées pour vous aider à classer les groupes de propriétés par ordre de priorité.
Propriétés personnalisées		Vous pouvez ajouter des propriétés personnalisées individuelles au lieu des groupes de propriétés.
	Nouveau	Ajoutez une propriété personnalisée individuelle et appliquez-la au Blueprint global.
	Nom	Entrez le nom de la propriété. Pour obtenir la liste des propriétés personnalisées et leurs définitions, reportez-vous à <i>Référence des propriétés personnalisées</i> .
	Valeur	Entrez la valeur de la propriété personnalisée.

Tableau 3-4. Paramètres de l'onglet Propriétés (suite)

Onglet	Configuration	Description
	Chiffré	Vous pouvez choisir de chiffrer la valeur de la propriété, par exemple, si la valeur est un mot de passe.
	Remplaçable	Vous pouvez spécifier que la valeur de la propriété peut être remplacée par la prochaine personne qui utilise la propriété. Il s'agit généralement d'un autre architecte, mais si vous sélectionnez Afficher dans la demande, vos utilisateurs peuvent voir et modifier les valeurs des propriétés lorsqu'ils demandent des éléments du catalogue.
	Afficher dans la demande	Si vous souhaitez afficher le nom et la valeur de la propriété pour vos utilisateurs finaux, vous pouvez indiquer d'afficher la propriété sur le formulaire de demande lors de la demande de provisionnement de machine. Vous pouvez également sélectionner Remplaçable si vous souhaitez que les utilisateurs fournissent une valeur.

Paramètres du composant de machine vSphere

Description des paramètres et des options que vous pouvez configurer pour un composant de machine vSphere dans le canevas de conception de Blueprint vRealize Automation. vSphere est le seul type de composant machine pouvant utiliser les paramètres du composant réseau et de sécurité NSX dans le canevas de conception.

Onglet Général

Configurez des paramètres généraux pour un composant de machine vSphere.

Tableau 3-5. Paramètres de l'onglet Général

Configuration	Description
ID	Entrez le nom du composant de votre machine ou acceptez le nom par défaut.
Description	Résumez le composant de votre machine à l'attention d'autres architectes.
Afficher l'emplacement à la demande	Dans un environnement cloud, tel que vCloud Air, cela permet aux utilisateurs de sélectionner une région pour leurs machines provisionnées. Pour un environnement virtuel, tel que vSphere, vous pouvez configurer la fonctionnalité des emplacements pour permettre aux utilisateurs de sélectionner un emplacement de centre de données particulier sur lequel provisionner une machine demandée. Pour configurer complètement cette option, un administrateur système ajoute les informations sur l'emplacement du centre de données dans un fichier d'emplacements et un administrateur Fabric modifie une ressource de calcul pour l'associer à un emplacement.

Tableau 3-5. Paramètres de l'onglet Général (suite)

Configuration	Description
Stratégie de réservation	<p>Appliquez une stratégie de réservation à un Blueprint de manière à restreindre à un sous-ensemble de réservations disponibles les machines provisionnées à partir de ce Blueprint. Les administrateurs Fabric créent des stratégies de réservation qui offrent un moyen facultatif et utile de contrôler le mode de traitement des demandes de réservation (par exemple, pour collecter des ressources auprès de groupes pour différents niveaux de services ou pour rendre un type de ressources particulier facilement disponible dans un but précis). Si votre administrateur Fabric n'a pas configuré des stratégies de réservation, vous ne voyez aucune option disponible dans ce menu déroulant.</p>
Préfixe de machine	<p>Des préfixes de machines sont créés par les administrateurs Fabric et sont utilisés pour créer les noms des machines provisionnées. Si vous sélectionnez Utiliser la valeur par défaut du groupe, les machines provisionnées à partir de votre Blueprint sont nommées selon le préfixe de machine configuré comme préfixe par défaut pour le groupe d'activité des utilisateurs. Si aucun préfixe de machine n'est configuré, un préfixe est généré pour vous en fonction du nom du groupe d'activité.</p> <p>Si votre administrateur Fabric configure d'autres préfixes de machines que vous devrez sélectionner, vous pouvez appliquer un préfixe à toutes les machines provisionnées à partir de votre Blueprint, quel que soit le demandeur.</p>
Instances : minimum et maximum	<p>Configurez le nombre maximal et minimal d'instances que les utilisateurs peuvent demander pour un déploiement ou pour une action de réduction de charge ou de montée en charge. Si vous ne souhaitez pas laisser de choix aux utilisateurs, l'entrée de la même valeur dans les champs Valeur minimale et Valeur maximale configure exactement le nombre d'instances à provisionner et désactive les actions de réduction et de montée en charge pour ce composant de la machine.</p> <p>Les composants XaaS ne sont pas évolutifs et ne sont pas mis à jour lors d'une opération de dimensionnement. Si vous utilisez des composants XaaS dans votre Blueprint, vous pouvez créer une action sur les ressources exécutée par les utilisateurs après une opération de dimensionnement, qui permette de dimensionner ou de mettre à jour vos composants XaaS. Vous pouvez aussi désactiver le dimensionnement en configurant exactement le nombre d'instances à autoriser par composant de machine.</p>

Onglet Informations sur le build

Configurez des paramètres d'informations de la build pour un composant de machine vSphere.

Tableau 3-6. Onglet Informations sur le build

Configuration	Description
Type de Blueprint	À des fins d'archivage et d'attribution de licence, déterminez si les machines provisionnées à partir de ce Blueprint sont classées comme Poste de travail ou comme Serveur.
Action	<p>Les options qui apparaissent dans le menu déroulant Action dépendent du type de machine que vous sélectionnez.</p> <p>Les actions suivantes sont disponibles :</p> <ul style="list-style-type: none"> ■ Créer <p>Créez la spécification du composant de machine sans utiliser d'option de clonage.</p> ■ Cloner <p>Réalisez des copies d'une machine virtuelle à l'aide d'un modèle et d'un objet de personnalisation.</p> ■ Clone lié <p>Provisionnez une copie de machine virtuelle disposant d'un espace suffisant appelée clone lié. Les clones liés sont basés sur un snapshot de machine virtuelle et utilisent une chaîne de disques delta pour effectuer le suivi des différences avec la machine parent.</p> <p>Le snapshot de machine virtuelle identifié dans le Blueprint doit être désactivé avant de provisionner les machines virtuelles de clones liés.</p> ■ NetApp FlexClone <p>Si vos administrateurs Fabric ont configuré vos réservations pour utiliser le stockage NetApp FlexClone, vous pouvez cloner des copies de machines à optimisation d'espace à l'aide de cette technologie.</p>

Tableau 3-6. Onglet Informations sur le build (suite)

Configuration	Description
Workflow de provisionnement	<p>Les options qui apparaissent dans le menu déroulant Workflow de provisionnement dépendent du type de machine et de l'action que vous sélectionnez.</p> <ul style="list-style-type: none"> ■ BasicVmWorkflow <p>Provisionnez une machine sans système d'exploitation invité.</p> ■ ExternalProvisioningWorkflow <p>Créez une machine en démarrant à partir d'une instance de machine virtuelle ou d'une image basée sur le cloud.</p> ■ LinuxKickstartWorkflow <p>Provisionnez une machine en effectuant un démarrage à partir d'une image ISO, à l'aide d'un fichier de configuration kickstart ou autoYaSt et une image de distribution Linux pour installer le système d'exploitation sur la machine.</p> ■ VirtualSccmProvisioningWorkflow <p>Provisionnez une machine et transmettez le contrôle à une séquence de tâches SCCM pour effectuer un démarrage à partir d'une image ISO, déployer un système d'exploitation Windows et installez l'agent invité vRealize Automation.</p> ■ WIMImageWorkflow <p>Provisionnez une machine en effectuant un démarrage dans un environnement WinPE et en installant un système d'exploitation à l'aide de l'image au format WIM d'une machine de référence Windows.</p> <p>Lors de l'utilisation d'un workflow de provisionnement WIM dans un Blueprint, spécifiez une valeur de stockage qui tient compte de la taille de chaque disque à utiliser sur la machine. Utilisez la valeur totale de tous les disques comme valeur de stockage minimale pour le composant de machine. Spécifiez également pour chaque disque une taille suffisante pour recevoir le système d'exploitation.</p>
Cloner à partir de	<p>Sélectionnez un modèle de machine à partir duquel vous pourrez effectuer le clonage. Vous pouvez affiner la liste des modèles disponibles à l'aide de l'option Filtres du menu déroulant de chaque colonne, par exemple, l'option de menu Filtres de la colonne Noms.</p> <p>Avec la méthode Clone lié, seules les machines ayant des snapshots disponibles pour le clonage et que vous gérez en tant qu'administrateur de locataire ou gestionnaire de groupe d'activité sont affichées.</p> <p>Vous ne pouvez cloner qu'à partir de modèles qui existent sur des machines que vous gérez en tant que gestionnaire de groupes d'activité ou Administrateur de locataires.</p>

Tableau 3-6. Onglet Informations sur le build (suite)

Configuration	Description
Cloner à partir d'un snapshot	<p>Avec la méthode Clone lié, sélectionnez un snapshot existant à partir duquel vous pourrez effectuer le clonage, sur la base du modèle de machine sélectionné. Les machines n'apparaissent dans la liste que si elles disposent déjà d'un snapshot et si vous gérez cette machine en tant qu'administrateur de locataire ou gestionnaire de groupe d'activité.</p> <p>Si vous sélectionnez Utiliser le snapshot actuel, le clone est défini avec des caractéristiques identiques au dernier état de la machine virtuelle. Si vous souhaitez effectuer un clonage par rapport à un snapshot réel, cliquez sur l'option du menu déroulant et sélectionnez le snapshot en question dans la liste.</p> <hr/> <p>Remarque Le terme snapshot peut prêter à confusion. Si vous sélectionnez un snapshot, l'option crée un disque dont le snapshot est un parent. L'option Utiliser le snapshot actuel ne comporte pas de disque de base pouvant être utilisé comme parent et exécute silencieusement une action de clone complet. En tant que palliatif, vous pouvez créer des snapshots sur le disque de base ou utiliser un workflow vRealize Orchestrator pour créer un snapshot, puis un clone à partir de ce snapshot.</p> <hr/> <p>Cette option est disponible uniquement pour l'action de clone lié.</p>
Spécification de personnalisation	<p>Spécifiez une spécification de personnalisation disponible. Une spécification de personnalisation est requise uniquement si vous clonez avec des adresses IP statiques.</p> <p>Vous ne pouvez pas réaliser de personnalisations de machines Windows sans une spécification de personnalisation. Pour les machines de clone Linux, vous pouvez effectuer une personnalisation en utilisant une spécification de personnalisation, un script externe ou les deux.</p>

Onglet Ressources de machine

Spécifiez les paramètres de CPU, de mémoire et de stockage du composant de machine vSphere.

Tableau 3-7. Onglet Ressources de machine

Configuration	Description
CPU : Valeur minimale et Valeur maximale	Entrez un nombre minimal et un nombre maximal de CPU pouvant être provisionnés par ce composant de machine.
Mémoire (Mo) : Valeur minimale et Valeur maximale	Entrez une quantité minimale et une quantité maximale de mémoire pouvant être consommées par des machines provisionnées par ce composant de machine.
Stockage (Go) : Valeur minimale et Valeur maximale	<p>Entrez une quantité minimale et une quantité maximale de stockage pouvant être consommées par des machines provisionnées par ce composant de machine. Pour vSphere, KVM (RHEV), SCVMM, vCloud Air et vCloud Director, la quantité de stockage minimale est définie en fonction de ce que vous avez entré dans l'onglet Stockage.</p> <p>Lors de l'utilisation d'un workflow de provisionnement WIM dans un Blueprint, spécifiez une valeur de stockage qui tient compte de la taille de chaque disque à utiliser sur la machine. Utilisez la valeur totale de tous les disques comme valeur de stockage minimale pour le composant de machine. Spécifiez également pour chaque disque une taille suffisante pour recevoir le système d'exploitation.</p>

Onglet Stockage

Vous pouvez ajouter des paramètres de volume de stockage, notamment une ou plusieurs stratégies de stockage, au composant de machine pour contrôler l'espace de stockage.

Tableau 3-8. Paramètres de l'onglet Stockage

Configuration	Description
ID	Entrez un ID ou un nom pour le volume de stockage.
Capacité (Go)	Entrez la capacité de stockage pour le volume de stockage.
Lettre de lecteur / Chemin de montage	Entrez une lettre de lecteur ou un chemin de montage pour le volume de stockage.
Étiquette	Entrez une étiquettes pour la lettre de lecteur et le chemin de montage du volume de stockage.
Stratégie de réservation de stockage	Entrez la stratégie de réservation de stockage existante à utiliser avec ce volume de stockage.
Propriétés personnalisées	Entrez des propriétés personnalisées à utiliser avec ce volume de stockage.
Nombre maximal de volumes	Entrez le nombre maximal de volumes de stockage autorisés pouvant être utilisés lors d'un provisionnement à partir du composant de machine. Entrez 0 pour empêcher d'autres personnes d'ajouter des volumes de stockage. La valeur par défaut est 60.
Autoriser l'utilisateur à voir et à modifier les stratégies de réservation de stockage	Cochez cette case pour permettre aux utilisateurs de supprimer une stratégie de réservation associée ou de spécifier une autre stratégie de réservation lors du provisionnement.

Onglet Réseau

Vous pouvez configurer des paramètres réseau pour un composant de machine vSphere sur la base de paramètres réseau et d'équilibrage de charge de NSX configurés à l'extérieur de vRealize Automation. Vous pouvez utiliser les paramètres d'un ou de plusieurs composants réseau NSX existants ou à la demande dans le canevas de conception.

Pour plus d'informations sur l'ajout et la configuration des composants réseau et de sécurité NSX avant d'utiliser les paramètres de l'onglet Réseau sur un composant de machine vSphere, reportez-vous à [Configuration des paramètres de composants de réseau et de sécurité](#).

Pour plus d'informations sur la spécification de paramètres NSX au niveau du Blueprint s'appliquant aux composants de machine vSphere, reportez-vous à [Paramètres de la page Nouveau Blueprint et Propriétés du Blueprint avec NSX](#).

Tableau 3-9. Paramètres de l'onglet Réseau

Configuration	Description
Réseau	Sélectionnez un composant réseau dans le menu déroulant. Seuls les composants réseau existant dans le canevas de conception sont répertoriés.
Type d'attribution	Acceptez l'attribution par défaut dérivé du composant réseau ou sélectionnez un type d'attribution dans le menu déroulant. Les valeurs des options DHCP et Statique sont dérivées des paramètres du composant réseau.
Adresse	Spécifiez l'adresse IP du réseau. Cette option est uniquement disponible pour le type d'adresse statique.
Équilibrage de charge	Entrez le service à utiliser pour l'équilibrage de charge.
Propriétés personnalisées	Affichez les propriétés personnalisées qui sont configurées pour le composant réseau ou le profil réseau sélectionné.
Nombre maximal d'adaptateurs réseau	Spécifiez le nombre maximal d'adaptateurs réseau, ou NIC, à autoriser pour ce composant de machine. Le nombre par défaut est illimité. Définissez cette option sur 0 pour désactiver l'ajout de cartes réseau pour les composants de machine.

Onglet Sécurité

Vous pouvez configurer des paramètres de sécurité pour un composant de machine vSphere sur la base de paramètres de NSX configurés à l'extérieur de vRealize Automation. Vous pouvez éventuellement utiliser les paramètres de composants de sécurité de NSX existants et à la demande dans le canevas de conception.

Les paramètres de sécurité d'un groupe de sécurité existant et à la demande et les composants de balise de sécurité dans le canevas de conception sont automatiquement disponibles.

Pour plus d'informations sur l'ajout et la configuration des composants réseau et de sécurité NSX avant d'utiliser les paramètres de l'onglet Sécurité sur un composant de machine vSphere, reportez-vous à [Configuration des paramètres de composants de réseau et de sécurité](#).

Pour plus d'informations sur la spécification des informations de NSX au niveau du Blueprint s'appliquant aux composants de machine vSphere, reportez-vous à [Paramètres de la page Nouveau Blueprint et Propriétés du Blueprint avec NSX](#).

Tableau 3-10. Paramètres de l'onglet Sécurité

Configuration	Description
Nom	Affichez le nom d'un groupe de sécurité ou d'une balise NSX. Les noms sont dérivés des composants de sécurité du canevas de conception. Cochez la case en regard d'une balise ou d'un groupe de sécurité répertorié pour utiliser ce groupe ou cette balise pour un provisionnement à partir de ce composant de machine.
Type	Indiquez si l'élément de sécurité est un groupe de sécurité à la demande, un groupe de sécurité existant ou une balise de sécurité.
Description	Affichez la description définie pour le groupe de sécurité ou la balise.
Point de terminaison	Affichez le point de terminaison utilisé par le groupe de sécurité ou la balise NSX.

Onglet Propriétés

En option, spécifiez des informations de propriété personnalisée et de groupe de propriétés pour votre composant de machine vSphere.

Vous pouvez ajouter des propriétés individuelles personnalisées et des groupes de propriétés personnalisées aux composants de machine en utilisant l'onglet **Propriétés**. Vous pouvez également ajouter des propriétés personnalisées et des groupes de propriétés personnalisées à l'aide de l'onglet **Propriétés** lorsque vous créez ou modifiez un Blueprint respectivement dans la page **Nouveau Blueprint** ou **Propriétés du Blueprint**.

Vous pouvez utiliser l'onglet **Propriétés personnalisées** pour ajouter et configurer des options pour des propriétés personnalisées existantes. Des propriétés personnalisées sont fournies avec vRealize Automation et vous pouvez également créer de nouvelles définitions de propriétés.

Tableau 3-11. Paramètres de l'onglet Propriétés > Propriétés personnalisées

Configuration	Description
Nom	Entrez le nom d'une propriété personnalisée ou sélectionnez une propriété personnalisée disponible dans le menu déroulant. Par exemple, entrez le nom de la propriété personnalisée <i>Machine.SSH</i> pour spécifier si les machines provisionnées à l'aide de ce Blueprint autorisent les connexions SSH. Les propriétés apparaissent dans le menu déroulant uniquement si votre administrateur de locataire ou votre administrateur Fabric a créé des définitions de propriétés.
Valeur	Entrez ou modifiez une valeur à associer au nom de la propriété personnalisée. Par exemple, définissez la valeur sur <i>true</i> pour permettre aux utilisateurs autorisés de se connecter via SSH à des machines provisionnées à l'aide de votre Blueprint.
Chiffré	Vous pouvez choisir de chiffrer la valeur de la propriété, par exemple, si la valeur est un mot de passe.
Remplaçable	Vous pouvez spécifier que la valeur de la propriété peut être remplacée par la prochaine personne qui utilise la propriété. Il s'agit généralement d'un autre architecte, mais si vous sélectionnez <i>Afficher</i> dans la demande, vos utilisateurs peuvent voir et modifier les valeurs des propriétés lorsqu'ils demandent des éléments du catalogue.
Afficher dans la demande	Si vous souhaitez afficher le nom et la valeur de la propriété pour vos utilisateurs finaux, vous pouvez indiquer d'afficher la propriété sur le formulaire de demande lors de la demande de provisionnement de machine. Vous pouvez également sélectionner <i>Remplaçable</i> si vous souhaitez que les utilisateurs fournissent une valeur.

Vous pouvez utiliser l'onglet **Groupes de propriétés** pour ajouter et configurer des paramètres pour des groupes de propriétés personnalisées existants. Vous pouvez créer vos propres groupes de propriétés ou utiliser des groupes de propriétés qui ont déjà été créés.

Tableau 3-12. Paramètres de l'onglet Propriétés > Groupes de propriétés

Configuration	Description
Nom	Sélectionnez un groupe de propriétés disponible dans le menu déroulant.
Monter et Descendre	Contrôlez le niveau de priorité des groupes de priorités répertoriés en ordre décroissant. Le premier groupe de propriétés répertorié a priorité sur le groupe de propriétés suivant, et ainsi de suite.

Tableau 3-12. Paramètres de l'onglet Propriétés > Groupes de propriétés (suite)

Configuration	Description
Afficher les propriétés	Affichez les propriétés personnalisées du groupe de propriétés sélectionné.
Afficher les propriétés fusionnées	Affichez toutes les propriétés personnalisées des groupes de propriétés répertoriés dans leur ordre d'affichage dans la liste de groupes de propriétés. Lorsque la même propriété figure dans plusieurs groupes de propriétés, le nom de la propriété figure une seule fois dans la liste selon la position où elle y est rencontrée en premier.

Onglet Profils

Les profils de composants permettent de paramétrer les Blueprints, par exemple, plutôt que de créer un Blueprint distinct, petit, moyen et grand. Vous pouvez créer un Blueprint unique avec une petite, moyenne et grande capacité, et activer votre capacité à sélectionner l'une des tailles lors du déploiement de l'élément du catalogue. Les profils de composants sont spécifiquement conçus pour réduire la prolifération de Blueprints et simplifier votre catalogue.

Si vous avez créé des ensembles de valeurs pour les profils de composants Size et Image de vRealize Automation fournis, vous pouvez ajouter et configurer ces paramètres pour le composant de machine dans le Blueprint. Vous pouvez également sélectionner une valeur différente définie au moment du déploiement de l'élément du catalogue.

Les profils de composants sont uniquement disponibles pour les composants de machine vSphere.

Lorsque vous ajoutez un profil de composant au composant de machine vSphere d'un Blueprint, les paramètres définis dans l'ensemble ou les ensembles de valeurs sélectionnés du profil remplacent les autres paramètres du composant de machine, tels que le nombre de CPU et le stockage.

L'ensemble de valeurs du profil de composant défini est appliqué à toutes les machines vSphere d'un cluster.

Vous ne pouvez pas reconfigurer les machines à l'aide des profils de composants Size ou Image, mais la plage de CPU, de la mémoire et du stockage qui est calculée en fonction du profil reste disponible pour des actions de reconfiguration. Par exemple, si vous avez utilisé un petit (1 CPU, 1 024 Mo de mémoire et 10 Go de stockage), moyen (3 CPU, 2 048 Mo de mémoire et 12 Go de stockage) et grand (5 CPU, 3 072 Mo de mémoire et 15 Go de stockage) ensemble de valeurs Size, les plages disponibles pendant la reconfiguration de la machine sont 1 à 5 CPU, 1 024 à 3 072 Mo de mémoire et 1 à 15 Go de stockage.

Pour plus d'informations sur la définition d'ensembles de valeurs pour les profils de composants, reportez-vous à la section *Référence des propriétés personnalisées*.

Tableau 3-13. Paramètres de l'onglet Profils

Configuration	Description
Ajouter	Ajoutez le profil de composant Size ou Image.
Modifier les ensembles de valeurs	Attribuez un ou plusieurs ensembles de valeurs pour le profil de composant sélectionné en choisissant parmi la liste des ensembles de valeurs définis. Vous pouvez sélectionner l'un des ensembles de valeurs par défaut.
Supprimer	Supprimez le profil de composant Size ou Image.

Paramètres du composant de machine vCloud Air

Description des paramètres et des options que vous pouvez configurer pour un composant de machine vCloud Air dans le canevas de conception de Blueprint vRealize Automation.

Onglet Général

Configurez des paramètres généraux pour un composant de machine vCloud Air.

Tableau 3-14. Paramètres de l'onglet Général

Configuration	Description
ID	Entrez le nom du composant de votre machine ou acceptez le nom par défaut.
Description	Résumez le composant de votre machine à l'attention d'autres architectes.
Afficher l'emplacement à la demande	Dans un environnement cloud, tel que vCloud Air, cela permet aux utilisateurs de sélectionner une région pour leurs machines provisionnées. Pour un environnement virtuel, tel que vSphere, vous pouvez configurer la fonctionnalité des emplacements pour permettre aux utilisateurs de sélectionner un emplacement de centre de données particulier sur lequel provisionner une machine demandée. Pour configurer complètement cette option, un administrateur système ajoute les informations sur l'emplacement du centre de données dans un fichier d'emplacements et un administrateur Fabric modifie une ressource de calcul pour l'associer à un emplacement.
Stratégie de réservation	Appliquez une stratégie de réservation à un Blueprint de manière à restreindre à un sous-ensemble de réservations disponibles les machines provisionnées à partir de ce Blueprint. Les administrateurs Fabric créent des stratégies de réservation qui offrent un moyen facultatif et utile de contrôler le mode de traitement des demandes de réservation (par exemple, pour collecter des ressources auprès de groupes pour différents niveaux de services ou pour rendre un type de ressources particulier facilement disponible dans un but précis). Si votre administrateur Fabric n'a pas configuré des stratégies de réservation, vous ne voyez aucune option disponible dans ce menu déroulant.

Tableau 3-14. Paramètres de l'onglet **Général** (suite)

Configuration	Description
Préfixe de machine	<p>Des préfixes de machines sont créés par les administrateurs Fabric et sont utilisés pour créer les noms des machines provisionnées. Si vous sélectionnez Utiliser la valeur par défaut du groupe, les machines provisionnées à partir de votre Blueprint sont nommées selon le préfixe de machine configuré comme préfixe par défaut pour le groupe d'activité des utilisateurs. Si aucun préfixe de machine n'est configuré, un préfixe est généré pour vous en fonction du nom du groupe d'activité.</p> <p>Si votre administrateur Fabric configure d'autres préfixes de machines que vous devrez sélectionner, vous pouvez appliquer un préfixe à toutes les machines provisionnées à partir de votre Blueprint, quel que soit le demandeur.</p>
Instances : minimum et maximum	<p>Configurez le nombre maximal et minimal d'instances que les utilisateurs peuvent demander pour un déploiement ou pour une action de réduction de charge ou de montée en charge. Si vous ne souhaitez pas laisser de choix aux utilisateurs, l'entrée de la même valeur dans les champs Valeur minimale et Valeur maximale configure exactement le nombre d'instances à provisionner et désactive les actions de réduction et de montée en charge pour ce composant de la machine.</p> <p>Les composants XaaS ne sont pas évolutifs et ne sont pas mis à jour lors d'une opération de dimensionnement. Si vous utilisez des composants XaaS dans votre Blueprint, vous pouvez créer une action sur les ressources exécutée par les utilisateurs après une opération de dimensionnement, qui permette de dimensionner ou de mettre à jour vos composants XaaS. Vous pouvez aussi désactiver le dimensionnement en configurant exactement le nombre d'instances à autoriser par composant de machine.</p>

Onglet Informations sur le build

Configurez des paramètres d'informations de la build pour un composant de machine vCloud Air.

Tableau 3-15. Onglet **Informations sur le build**

Configuration	Description
Type de Blueprint	À des fins d'archivage et d'attribution de licence, déterminez si les machines provisionnées à partir de ce Blueprint sont classées comme Poste de travail ou comme Serveur.
Action	<p>Les options qui apparaissent dans le menu déroulant Action dépendent du type de machine que vous sélectionnez.</p> <p>La seule action de provisionnement disponible pour un composant de machine vCloud Air est Cloner.</p> <ul style="list-style-type: none"> ■ Cloner <p>Réalisez des copies d'une machine virtuelle à l'aide d'un modèle et d'un objet de personnalisation.</p>

Tableau 3-15. Onglet Informations sur le build (suite)

Configuration	Description
Workflow de provisionnement	<p>Les options qui apparaissent dans le menu déroulant Workflow de provisionnement dépendent du type de machine et de l'action que vous sélectionnez.</p> <p>La seule action de provisionnement disponible pour un composant de machine vCloud Air est Cloner le workflow.</p> <ul style="list-style-type: none"> ■ CloneWorkflow <p>Réalisez des copies d'une machine virtuelle, en utilisant la méthode Clone, Clone lié ou Netapp FlexCone.</p>
Cloner à partir de	<p>Sélectionnez un modèle de machine à partir duquel vous pourrez effectuer le clonage. Vous pouvez affiner la liste des modèles disponibles à l'aide de l'option Filtres du menu déroulant de chaque colonne, par exemple, l'option de menu Filtres de la colonne Noms.</p> <p>Avec la méthode Clone lié, seules les machines ayant des snapshots disponibles pour le clonage et que vous gérez en tant qu'administrateur de locataire ou gestionnaire de groupe d'activité sont affichées.</p> <p>Vous ne pouvez cloner qu'à partir de modèles qui existent sur des machines que vous gérez en tant que gestionnaire de groupes d'activité ou Administrateur de locataires.</p>

Onglet Ressources de machine

Spécifiez les paramètres de CPU, de mémoire et de stockage pour votre composant de machine vCloud Air.

Tableau 3-16. Onglet Ressources de machine

Configuration	Description
CPU : Valeur minimale et Valeur maximale	Entrez un nombre minimal et un nombre maximal de CPU pouvant être provisionnés par ce composant de machine.
Mémoire (Mo) : Valeur minimale et Valeur maximale	Entrez une quantité minimale et une quantité maximale de mémoire pouvant être consommées par des machines provisionnées par ce composant de machine.
Stockage (Go) : Valeur minimale et Valeur maximale	Entrez une quantité minimale et une quantité maximale de stockage pouvant être consommées par des machines provisionnées par ce composant de machine. Pour vSphere, KVM (RHEV), SCVMM, vCloud Air et vCloud Director, la quantité de stockage minimale est définie en fonction de ce que vous avez entré dans l'onglet Stockage.

Onglet Stockage

Vous pouvez ajouter des paramètres de volume de stockage, notamment une ou plusieurs stratégies de stockage, au composant de machine pour contrôler l'espace de stockage.

Tableau 3-17. Paramètres de l'onglet Stockage

Configuration	Description
ID	Entrez un ID ou un nom pour le volume de stockage.
Capacité (Go)	Entrez la capacité de stockage pour le volume de stockage.
Lettre de lecteur / Chemin de montage	Entrez une lettre de lecteur ou un chemin de montage pour le volume de stockage.
Étiquette	Entrez une étiquettes pour la lettre de lecteur et le chemin de montage du volume de stockage.
Stratégie de réservation de stockage	Entrez la stratégie de réservation de stockage existante à utiliser avec ce volume de stockage.
Propriétés personnalisées	Entrez des propriétés personnalisées à utiliser avec ce volume de stockage.
Nombre maximal de volumes	Entrez le nombre maximal de volumes de stockage autorisés pouvant être utilisés lors d'un provisionnement à partir du composant de machine. Entrez 0 pour empêcher d'autres personnes d'ajouter des volumes de stockage. La valeur par défaut est 60.
Autoriser l'utilisateur à voir et à modifier les stratégies de réservation de stockage	Cochez cette case pour permettre aux utilisateurs de supprimer une stratégie de réservation associée ou de spécifier une autre stratégie de réservation lors du provisionnement.

Onglet Propriétés

En option, spécifiez des informations de propriété personnalisée et de groupe de propriétés pour votre composant de machine vCloud Air.

Vous pouvez ajouter des propriétés individuelles personnalisées et des groupes de propriétés personnalisées aux composants de machine en utilisant l'onglet **Propriétés**. Vous pouvez également ajouter des propriétés personnalisées et des groupes de propriétés personnalisées à l'aide de l'onglet **Propriétés** lorsque vous créez ou modifiez un Blueprint respectivement dans la page **Nouveau Blueprint** ou **Propriétés du Blueprint**.

Vous pouvez utiliser l'onglet **Propriétés personnalisées** pour ajouter et configurer des options pour des propriétés personnalisées existantes. Des propriétés personnalisées sont fournies avec vRealize Automation et vous pouvez également créer de nouvelles définitions de propriétés.

Tableau 3-18. Paramètres de l'onglet Propriétés > Propriétés personnalisées

Configuration	Description
Nom	Entrez le nom d'une propriété personnalisée ou sélectionnez une propriété personnalisée disponible dans le menu déroulant. Par exemple, entrez le nom de la propriété personnalisée <i>Machine.SSH</i> pour spécifier si les machines provisionnées à l'aide de ce Blueprint autorisent les connexions SSH. Les propriétés apparaissent dans le menu déroulant uniquement si votre administrateur de locataire ou votre administrateur Fabric a créé des définitions de propriétés.
Valeur	Entrez ou modifiez une valeur à associer au nom de la propriété personnalisée. Par exemple, définissez la valeur sur <i>true</i> pour permettre aux utilisateurs autorisés de se connecter via SSH à des machines provisionnées à l'aide de votre Blueprint.
Chiffré	Vous pouvez choisir de chiffrer la valeur de la propriété, par exemple, si la valeur est un mot de passe.
Remplaçable	Vous pouvez spécifier que la valeur de la propriété peut être remplacée par la prochaine personne qui utilise la propriété. Il s'agit généralement d'un autre architecte, mais si vous sélectionnez <i>Afficher</i> dans la demande, vos utilisateurs peuvent voir et modifier les valeurs des propriétés lorsqu'ils demandent des éléments du catalogue.
Afficher dans la demande	Si vous souhaitez afficher le nom et la valeur de la propriété pour vos utilisateurs finaux, vous pouvez indiquer d'afficher la propriété sur le formulaire de demande lors de la demande de provisionnement de machine. Vous pouvez également sélectionner <i>Remplaçable</i> si vous souhaitez que les utilisateurs fournissent une valeur.

Vous pouvez utiliser l'onglet **Groupes de propriétés** pour ajouter et configurer des paramètres pour des groupes de propriétés personnalisées existants. Vous pouvez créer vos propres groupes de propriétés ou utiliser des groupes de propriétés qui ont déjà été créés.

Tableau 3-19. Paramètres de l'onglet Propriétés > Groupes de propriétés

Configuration	Description
Nom	Sélectionnez un groupe de propriétés disponible dans le menu déroulant.
Monter et Descendre	Contrôlez le niveau de priorité des groupes de priorités répertoriés en ordre décroissant. Le premier groupe de propriétés répertorié a priorité sur le groupe de propriétés suivant, et ainsi de suite.

Tableau 3-19. Paramètres de l'onglet Propriétés > Groupes de propriétés (suite)

Configuration	Description
Afficher les propriétés	Affichez les propriétés personnalisées du groupe de propriétés sélectionné.
Afficher les propriétés fusionnées	Affichez toutes les propriétés personnalisées des groupes de propriétés répertoriés dans leur ordre d'affichage dans la liste de groupes de propriétés. Lorsque la même propriété figure dans plusieurs groupes de propriétés, le nom de la propriété figure une seule fois dans la liste selon la position où elle y est rencontrée en premier.

Paramètres de composants de machines Amazon

Apprenez le fonctionnement des paramètres et des options que vous pouvez configurer pour un composant de machine Amazon dans le canevas de conception de Blueprint de vRealize Automation.

Onglet Général

Configurez les paramètres généraux d'un composant de machine Amazon.

Tableau 3-20. Paramètres de l'onglet Général

Configuration	Description
ID	Entrez le nom du composant de votre machine ou acceptez le nom par défaut.
Description	Résumez le composant de votre machine à l'attention d'autres architectes.
Afficher l'emplacement à la demande	Dans un environnement cloud, tel que vCloud Air, cela permet aux utilisateurs de sélectionner une région pour leurs machines provisionnées. Pour un environnement virtuel, tel que vSphere, vous pouvez configurer la fonctionnalité des emplacements pour permettre aux utilisateurs de sélectionner un emplacement de centre de données particulier sur lequel provisionner une machine demandée. Pour configurer complètement cette option, un administrateur système ajoute les informations sur l'emplacement du centre de données dans un fichier d'emplacements et un administrateur Fabric modifie une ressource de calcul pour l'associer à un emplacement.
Stratégie de réservation	Appliquez une stratégie de réservation à un Blueprint de manière à restreindre à un sous-ensemble de réservations disponibles les machines provisionnées à partir de ce Blueprint. Les administrateurs Fabric créent des stratégies de réservation qui offrent un moyen facultatif et utile de contrôler le mode de traitement des demandes de réservation (par exemple, pour collecter des ressources auprès de groupes pour différents niveaux de services ou pour rendre un type de ressources particulier facilement disponible dans un but précis). Si votre administrateur Fabric n'a pas configuré des stratégies de réservation, vous ne voyez aucune option disponible dans ce menu déroulant.

Tableau 3-20. Paramètres de l'onglet **Général** (suite)

Configuration	Description
Préfixe de machine	<p>Des préfixes de machines sont créés par les administrateurs Fabric et sont utilisés pour créer les noms des machines provisionnées. Si vous sélectionnez Utiliser la valeur par défaut du groupe, les machines provisionnées à partir de votre Blueprint sont nommées selon le préfixe de machine configuré comme préfixe par défaut pour le groupe d'activité des utilisateurs. Si aucun préfixe de machine n'est configuré, un préfixe est généré pour vous en fonction du nom du groupe d'activité.</p> <p>Si votre administrateur Fabric configure d'autres préfixes de machines que vous devrez sélectionner, vous pouvez appliquer un préfixe à toutes les machines provisionnées à partir de votre Blueprint, quel que soit le demandeur.</p>
Instances : minimum et maximum	<p>Configurez le nombre maximal et minimal d'instances que les utilisateurs peuvent demander pour un déploiement ou pour une action de réduction de charge ou de montée en charge. Si vous ne souhaitez pas laisser de choix aux utilisateurs, l'entrée de la même valeur dans les champs Valeur minimale et Valeur maximale configure exactement le nombre d'instances à provisionner et désactive les actions de réduction et de montée en charge pour ce composant de la machine.</p> <p>Les composants XaaS ne sont pas évolutifs et ne sont pas mis à jour lors d'une opération de dimensionnement. Si vous utilisez des composants XaaS dans votre Blueprint, vous pouvez créer une action sur les ressources exécutée par les utilisateurs après une opération de dimensionnement, qui permette de dimensionner ou de mettre à jour vos composants XaaS. Vous pouvez aussi désactiver le dimensionnement en configurant exactement le nombre d'instances à autoriser par composant de machine.</p>

Onglet Informations sur le build

Configurez les paramètres d'information sur le build d'un composant de machine Amazon.

Tableau 3-21. Onglet Informations sur le build

Configuration	Description
Type de Blueprint	À des fins d'archivage et d'attribution de licence, déterminez si les machines provisionnées à partir de ce Blueprint sont classées comme Poste de travail ou comme Serveur.
Workflow de provisionnement	<p>Le seul workflow de provisionnement disponible pour un composant de machine Amazon est CloudProvisioningWorkflow.</p> <ul style="list-style-type: none"> ■ CloudProvisioningWorkflow <p>Créez une machine en démarrant à partir d'une instance de machine virtuelle ou d'une image basée sur le cloud.</p>

Tableau 3-21. Onglet Informations sur le build (suite)

Configuration	Description
Image de la machine Amazon	<p>Sélectionnez une image de machine Amazon disponible. Une image de machine Amazon est un modèle contenant une configuration logicielle, notamment un système d'exploitation. Les images de machine sont gérées par des comptes d'Amazon Web Services. Vous pouvez affiner la liste de noms d'images de machine Amazon à l'aide de l'option Filtres du menu déroulant de la colonne ID d'AMI.</p>
Paire de clés	<p>Les paires de clés sont requises pour un provisionnement avec Amazon Web Services.</p> <p>Les paires de clés permettent d'effectuer des provisionnements et de se connecter à une instance de cloud. Elles sont également utilisées pour déchiffrer des mots de passe Windows et pour se connecter à une machine Linux.</p> <p>Les options de paires de clés suivantes sont disponibles :</p> <ul style="list-style-type: none"> ■ Non spécifiée <p>Permet de contrôler le comportement d'une paire de clés au niveau du Blueprint plutôt qu'au niveau de la réservation.</p> ■ Générée automatiquement par groupe d'activité <p>Spécifie que chaque machine provisionnée dans le même groupe d'activité dispose d'une paire de clés identique, y compris les machines provisionnées sur d'autres réservations si elles disposent des mêmes ressources de calcul et groupe d'activité. Du fait que les paires de clés sont associées à un groupe d'activité, elles sont supprimées en même temps que le groupe d'activité.</p> ■ Générée automatiquement par machine <p>Spécifie que chaque machine dispose d'une paire de clés unique. L'option Générée automatiquement par machine est la plus sécurisée, car aucune paire de clés n'est partagée entre les machines.</p>
Activer les options réseau Amazon sur la machine	<p>Choisissez s'il convient de permettre aux utilisateurs de provisionner une machine dans un Virtual Private Cloud (VPC) ou un emplacement autre que VPC lorsqu'ils soumettent la demande.</p>
Types d'instances	<p>Sélectionnez un ou plusieurs types d'instances Amazon. Une instance Amazon est un serveur virtuel pouvant exécuter des applications dans Amazon Web Services. Les instances sont créées à partir d'une image de machine Amazon et en choisissant un type d'instance approprié. vRealize Automation gère les types d'instances d'images de machines disponibles pour le provisionnement.</p> <p>Pour obtenir des informations sur l'utilisation des types d'instances Amazon dans vRealize Automation, reportez-vous à Présentation des types d'instances d'Amazon et Ajouter un type d'instance Amazon.</p>

Onglet Ressources de machine

Spécifiez les paramètres de CPU, de mémoire, de stockage et de volume EBS pour votre composant de machine Amazon.

Vous pouvez également reconfigurer tous les volumes de stockage de la machine Amazon dans le déploiement à l'exception du volume racine.

Tableau 3-22. Onglet Ressources de machine

Configuration	Description
CPU : Valeur minimale et Valeur maximale	Entrez un nombre minimal et un nombre maximal de CPU pouvant être provisionnés par ce composant de machine.
Mémoire (Mo) : Valeur minimale et Valeur maximale	Entrez une quantité minimale et une quantité maximale de mémoire pouvant être consommées par des machines provisionnées par ce composant de machine.
Stockage (Go) : Valeur minimale et Valeur maximale	Entrez une quantité minimale et une quantité maximale de stockage pouvant être consommées par des machines provisionnées par ce composant de machine. Pour vSphere, KVM (RHEV), SCVMM, vCloud Air et vCloud Director, la quantité de stockage minimale est définie en fonction de ce que vous avez entré dans l'onglet Stockage.
Stockage EBS (Go) : Valeur minimale et Valeur maximale	Entrez un volume minimal et un volume maximal de stockage Amazon Elastic Block Store (EBS) pouvant être consommés par des ressources de machines provisionnées par ce composant de machine. Lors de la destruction d'un déploiement contenant un composant de machine Amazon, tous les volumes EBS ajoutés à la machine pendant son cycle de vie sont détachés plutôt que détruits. vRealize Automation ne propose pas d'option permettant de détruire les volumes EBS.

Onglet Propriétés

Facultativement, spécifiez des informations de propriétés et de groupe de propriétés personnalisées pour votre composant de machine Amazon.

Vous pouvez ajouter des propriétés individuelles personnalisées et des groupes de propriétés personnalisées aux composants de machine en utilisant l'onglet **Propriétés**. Vous pouvez également ajouter des propriétés personnalisées et des groupes de propriétés personnalisées à l'aide de l'onglet **Propriétés** lorsque vous créez ou modifiez un Blueprint respectivement dans la page **Nouveau Blueprint** ou **Propriétés du Blueprint**.

Vous pouvez utiliser l'onglet **Propriétés personnalisées** pour ajouter et configurer des options pour des propriétés personnalisées existantes. Des propriétés personnalisées sont fournies avec vRealize Automation et vous pouvez également créer de nouvelles définitions de propriétés.

Tableau 3-23. Paramètres de l'onglet Propriétés > Propriétés personnalisées

Configuration	Description
Nom	Entrez le nom d'une propriété personnalisée ou sélectionnez une propriété personnalisée disponible dans le menu déroulant. Par exemple, entrez le nom de la propriété personnalisée <code>Machine.SSH</code> pour spécifier si les machines provisionnées à l'aide de ce Blueprint autorisent les connexions SSH. Les propriétés apparaissent dans le menu déroulant uniquement si votre administrateur de locataire ou votre administrateur Fabric a créé des définitions de propriétés.
Valeur	Entrez ou modifiez une valeur à associer au nom de la propriété personnalisée. Par exemple, définissez la valeur sur <code>true</code> pour permettre aux utilisateurs autorisés de se connecter via SSH à des machines provisionnées à l'aide de votre Blueprint.
Chiffré	Vous pouvez choisir de chiffrer la valeur de la propriété, par exemple, si la valeur est un mot de passe.
Remplaçable	Vous pouvez spécifier que la valeur de la propriété peut être remplacée par la prochaine personne qui utilise la propriété. Il s'agit généralement d'un autre architecte, mais si vous sélectionnez <code>Afficher</code> dans la demande, vos utilisateurs peuvent voir et modifier les valeurs des propriétés lorsqu'ils demandent des éléments du catalogue.
Afficher dans la demande	Si vous souhaitez afficher le nom et la valeur de la propriété pour vos utilisateurs finaux, vous pouvez indiquer d'afficher la propriété sur le formulaire de demande lors de la demande de provisionnement de machine. Vous pouvez également sélectionner <code>Remplaçable</code> si vous souhaitez que les utilisateurs fournissent une valeur.

Vous pouvez utiliser l'onglet **Groupes de propriétés** pour ajouter et configurer des paramètres pour des groupes de propriétés personnalisées existants. Vous pouvez créer vos propres groupes de propriétés ou utiliser des groupes de propriétés qui ont déjà été créés.

Tableau 3-24. Paramètres de l'onglet Propriétés > Groupes de propriétés

Configuration	Description
Nom	Sélectionnez un groupe de propriétés disponible dans le menu déroulant.
Monter et Descendre	Contrôlez le niveau de priorité des groupes de propriétés répertoriés en ordre décroissant. Le premier groupe de propriétés répertorié a priorité sur le groupe de propriétés suivant, et ainsi de suite.

Tableau 3-24. Paramètres de l'onglet Propriétés > Groupes de propriétés (suite)

Configuration	Description
Afficher les propriétés	Affichez les propriétés personnalisées du groupe de propriétés sélectionné.
Afficher les propriétés fusionnées	Affichez toutes les propriétés personnalisées des groupes de propriétés répertoriés dans leur ordre d'affichage dans la liste de groupes de propriétés. Lorsque la même propriété figure dans plusieurs groupes de propriétés, le nom de la propriété figure une seule fois dans la liste selon la position où elle y est rencontrée en premier.

Paramètres de composant de machine OpenStack

Description des paramètres et options que vous pouvez configurer pour un composant de machine OpenStack dans le canevas de conception de Blueprint vRealize Automation.

Onglet Général

Configurez des paramètres généraux pour un composant de machine OpenStack.

Tableau 3-25. Paramètres de l'onglet Général

Configuration	Description
ID	Entrez le nom du composant de votre machine ou acceptez le nom par défaut.
Description	Résumez le composant de votre machine à l'attention d'autres architectes.
Afficher l'emplacement à la demande	Dans un environnement cloud, tel que vCloud Air, cela permet aux utilisateurs de sélectionner une région pour leurs machines provisionnées. Pour un environnement virtuel, tel que vSphere, vous pouvez configurer la fonctionnalité des emplacements pour permettre aux utilisateurs de sélectionner un emplacement de centre de données particulier sur lequel provisionner une machine demandée. Pour configurer complètement cette option, un administrateur système ajoute les informations sur l'emplacement du centre de données dans un fichier d'emplacements et un administrateur Fabric modifie une ressource de calcul pour l'associer à un emplacement.
Stratégie de réservation	Appliquez une stratégie de réservation à un Blueprint de manière à restreindre à un sous-ensemble de réservations disponibles les machines provisionnées à partir de ce Blueprint. Les administrateurs Fabric créent des stratégies de réservation qui offrent un moyen facultatif et utile de contrôler le mode de traitement des demandes de réservation (par exemple, pour collecter des ressources auprès de groupes pour différents niveaux de services ou pour rendre un type de ressources particulier facilement disponible dans un but précis). Si votre administrateur Fabric n'a pas configuré des stratégies de réservation, vous ne voyez aucune option disponible dans ce menu déroulant.

Tableau 3-25. Paramètres de l'onglet Général (suite)

Configuration	Description
Préfixe de machine	<p>Des préfixes de machines sont créés par les administrateurs Fabric et sont utilisés pour créer les noms des machines provisionnées. Si vous sélectionnez Utiliser la valeur par défaut du groupe, les machines provisionnées à partir de votre Blueprint sont nommées selon le préfixe de machine configuré comme préfixe par défaut pour le groupe d'activité des utilisateurs. Si aucun préfixe de machine n'est configuré, un préfixe est généré pour vous en fonction du nom du groupe d'activité.</p> <p>Si votre administrateur Fabric configure d'autres préfixes de machines que vous devrez sélectionner, vous pouvez appliquer un préfixe à toutes les machines provisionnées à partir de votre Blueprint, quel que soit le demandeur.</p>
Instances : minimum et maximum	<p>Configurez le nombre maximal et minimal d'instances que les utilisateurs peuvent demander pour un déploiement ou pour une action de réduction de charge ou de montée en charge. Si vous ne souhaitez pas laisser de choix aux utilisateurs, l'entrée de la même valeur dans les champs Valeur minimale et Valeur maximale configure exactement le nombre d'instances à provisionner et désactive les actions de réduction et de montée en charge pour ce composant de la machine.</p> <p>Les composants XaaS ne sont pas évolutifs et ne sont pas mis à jour lors d'une opération de dimensionnement. Si vous utilisez des composants XaaS dans votre Blueprint, vous pouvez créer une action sur les ressources exécutée par les utilisateurs après une opération de dimensionnement, qui permette de dimensionner ou de mettre à jour vos composants XaaS. Vous pouvez aussi désactiver le dimensionnement en configurant exactement le nombre d'instances à autoriser par composant de machine.</p>

Onglet Informations sur le build

Configurez des paramètres d'informations de la build pour un composant de machine OpenStack.

Tableau 3-26. Onglet Informations sur le build

Configuration	Description
Type de Blueprint	À des fins d'archivage et d'attribution de licence, déterminez si les machines provisionnées à partir de ce Blueprint sont classées comme Poste de travail ou comme Serveur.
Workflow de provisionnement	<p>Les workflows de provisionnement suivants sont disponibles pour un composant de machine OpenStack :</p> <ul style="list-style-type: none"> ■ CloudLinuxKickstartWorkflow Provisionnez une machine en effectuant un démarrage à partir d'une image ISO, à l'aide d'un fichier de configuration kickstart ou autoYaSt et une image de distribution Linux pour installer le système d'exploitation sur la machine. ■ CloudProvisioningWorkflow Créez une machine en démarrant à partir d'une instance de machine virtuelle ou d'une image basée sur le cloud. ■ CloudWIMImageWorkflow Provisionnez une machine en effectuant un démarrage dans un environnement WinPE et en installant un système d'exploitation à l'aide de l'image au format WIM d'une machine de référence Windows. Lors de l'utilisation d'un workflow de provisionnement WIM dans un Blueprint, spécifiez une valeur de stockage qui tient compte de la taille de chaque disque à utiliser sur la machine. Utilisez la valeur totale de tous les disques comme valeur de stockage minimale pour le composant de machine. Spécifiez également pour chaque disque une taille suffisante pour recevoir le système d'exploitation.
Image OpenStack	Sélectionnez une image OpenStack disponible. Une image OpenStack est un modèle contenant une configuration logicielle, notamment un système d'exploitation. Les images sont gérées par des comptes OpenStack. Vous pouvez affiner la liste de noms d'images OpenStack à l'aide de l'option Filtres du menu déroulant de la colonne Noms .

Tableau 3-26. Onglet Informations sur le build (suite)

Configuration	Description
Paire de clés	<p>Les paires de clés sont facultatives pour un provisionnement avec OpenStack.</p> <p>Les paires de clés permettent d'effectuer des provisionnements et de se connecter à une instance de cloud. Elles sont également utilisées pour déchiffrer des mots de passe Windows et pour se connecter à une machine Linux.</p> <p>Les options de paires de clés suivantes sont disponibles :</p> <ul style="list-style-type: none"> ■ Non spécifiée <p>Permet de contrôler le comportement d'une paire de clés au niveau du Blueprint plutôt qu'au niveau de la réservation.</p> ■ Générée automatiquement par groupe d'activité <p>Spécifie que chaque machine provisionnée dans le même groupe d'activité dispose d'une paire de clés identique, y compris les machines provisionnées sur d'autres réservations si elles disposent des mêmes ressources de calcul et groupe d'activité. Du fait que les paires de clés sont associées à un groupe d'activité, elles sont supprimées en même temps que le groupe d'activité.</p> ■ Générée automatiquement par machine <p>Spécifie que chaque machine dispose d'une paire de clés unique. L'option Générée automatiquement par machine est la plus sécurisée, car aucune paire de clés n'est partagée entre les machines.</p>
Types	<p>Sélectionnez un ou plusieurs types OpenStack. Un type OpenStack est un modèle de matériel virtuel définissant les spécifications de ressources de la machine pour des instances provisionnées dans OpenStack. Les types sont gérés dans le fournisseur OpenStack et sont importés pendant la collecte de données.</p>

Onglet Ressources de machine

Spécifiez les paramètres de CPU, de mémoire et de stockage pour votre composant de machine OpenStack.

Tableau 3-27. Onglet Ressources de machine

Configuration	Description
CPU : Valeur minimale et Valeur maximale	Entrez un nombre minimal et un nombre maximal de CPU pouvant être provisionnés par ce composant de machine.
Mémoire (Mo) : Valeur minimale et Valeur maximale	Entrez une quantité minimale et une quantité maximale de mémoire pouvant être consommées par des machines provisionnées par ce composant de machine.
Stockage (Go) : Valeur minimale et Valeur maximale	<p>Entrez une quantité minimale et une quantité maximale de stockage pouvant être consommées par des machines provisionnées par ce composant de machine. Pour vSphere, KVM (RHEV), SCVMM, vCloud Air et vCloud Director, la quantité de stockage minimale est définie en fonction de ce que vous avez entré dans l'onglet Stockage.</p> <p>Lors de l'utilisation d'un workflow de provisionnement WIM dans un Blueprint, spécifiez une valeur de stockage qui tient compte de la taille de chaque disque à utiliser sur la machine. Utilisez la valeur totale de tous les disques comme valeur de stockage minimale pour le composant de machine. Spécifiez également pour chaque disque une taille suffisante pour recevoir le système d'exploitation.</p>

Onglet Propriétés

En option, vous pouvez spécifier des informations de propriété personnalisée et de groupe de propriétés pour votre composant de machine OpenStack.

Vous pouvez ajouter des propriétés individuelles personnalisées et des groupes de propriétés personnalisées aux composants de machine en utilisant l'onglet **Propriétés**. Vous pouvez également ajouter des propriétés personnalisées et des groupes de propriétés personnalisées à l'aide de l'onglet **Propriétés** lorsque vous créez ou modifiez un Blueprint respectivement dans la page **Nouveau Blueprint** ou **Propriétés du Blueprint**.

Vous pouvez utiliser l'onglet **Propriétés personnalisées** pour ajouter et configurer des options pour des propriétés personnalisées existantes. Des propriétés personnalisées sont fournies avec vRealize Automation et vous pouvez également créer de nouvelles définitions de propriétés.

Tableau 3-28. Paramètres de l'onglet Propriétés > Propriétés personnalisées

Configuration	Description
Nom	Entrez le nom d'une propriété personnalisée ou sélectionnez une propriété personnalisée disponible dans le menu déroulant. Par exemple, entrez le nom de la propriété personnalisée <i>Machine.SSH</i> pour spécifier si les machines provisionnées à l'aide de ce Blueprint autorisent les connexions SSH. Les propriétés apparaissent dans le menu déroulant uniquement si votre administrateur de locataire ou votre administrateur Fabric a créé des définitions de propriétés.
Valeur	Entrez ou modifiez une valeur à associer au nom de la propriété personnalisée. Par exemple, définissez la valeur sur <i>true</i> pour permettre aux utilisateurs autorisés de se connecter via SSH à des machines provisionnées à l'aide de votre Blueprint.
Chiffré	Vous pouvez choisir de chiffrer la valeur de la propriété, par exemple, si la valeur est un mot de passe.
Remplaçable	Vous pouvez spécifier que la valeur de la propriété peut être remplacée par la prochaine personne qui utilise la propriété. Il s'agit généralement d'un autre architecte, mais si vous sélectionnez <i>Afficher</i> dans la demande, vos utilisateurs peuvent voir et modifier les valeurs des propriétés lorsqu'ils demandent des éléments du catalogue.
Afficher dans la demande	Si vous souhaitez afficher le nom et la valeur de la propriété pour vos utilisateurs finaux, vous pouvez indiquer d'afficher la propriété sur le formulaire de demande lors de la demande de provisionnement de machine. Vous pouvez également sélectionner <i>Remplaçable</i> si vous souhaitez que les utilisateurs fournissent une valeur.

Vous pouvez utiliser l'onglet **Groupes de propriétés** pour ajouter et configurer des paramètres pour des groupes de propriétés personnalisées existants. Vous pouvez créer vos propres groupes de propriétés ou utiliser des groupes de propriétés qui ont déjà été créés.

Tableau 3-29. Paramètres de l'onglet Propriétés > Groupes de propriétés

Configuration	Description
Nom	Sélectionnez un groupe de propriétés disponible dans le menu déroulant.
Monter et Descendre	Contrôlez le niveau de priorité des groupes de propriétés répertoriés en ordre décroissant. Le premier groupe de propriétés répertorié a priorité sur le groupe de propriétés suivant, et ainsi de suite.

Tableau 3-29. Paramètres de l'onglet Propriétés > Groupes de propriétés (suite)

Configuration	Description
Afficher les propriétés	Affichez les propriétés personnalisées du groupe de propriétés sélectionné.
Afficher les propriétés fusionnées	Affichez toutes les propriétés personnalisées des groupes de propriétés répertoriés dans leur ordre d'affichage dans la liste de groupes de propriétés. Lorsque la même propriété figure dans plusieurs groupes de propriétés, le nom de la propriété figure une seule fois dans la liste selon la position où elle y est rencontrée en premier.

Utilisation de propriétés réseau personnalisées

Vous pouvez spécifier des informations de réseau et de sécurité pour les composants de machine autres que vSphere et les Blueprints qui ne contiennent pas NSX en utilisant des propriétés réseau personnalisées au niveau du Blueprint ou du composant de machine.

Les composants **Réseau et sécurité** peuvent être utilisés uniquement avec les composants de machine vSphere. Les composants de machine autres que vSphere ne contiennent pas d'onglet **Réseau** ou **Sécurité**.

Pour les composants de machine ne disposant pas d'un onglet **Réseau** ou **Sécurité**, vous pouvez ajouter des propriétés personnalisées réseau et de sécurité telles que `VirtualMachine.Network0.Name` à leur onglet **Propriétés** dans le canevas de conception. Les propriétés de réseau, de sécurité et d'équilibrage de charge NSX s'appliquent uniquement aux machines vSphere.

Vous pouvez définir des propriétés personnalisées individuellement ou dans le cadre d'un groupe de propriétés existant via l'onglet **Propriétés** lorsque vous configurez un composant de machine dans le canevas de conception. Les propriétés personnalisées que vous définissez pour un composant de machine concernent des machines de ce type qui sont provisionnées à partir du Blueprint.

Pour plus d'informations sur les propriétés personnalisées disponibles, reportez-vous à *Référence des propriétés personnalisées*.

Résolution des problèmes de Blueprints pour les clones et clones liés

Lors de la création d'un Blueprint de clone lié ou de clone, une machine ou des modèles sont manquants. L'utilisation de votre Blueprint de clone partagé pour demander des machines échoue à provisionner des machines.

Problème

Lorsque vous travaillez avec des Blueprints de clones ou de clones liés, vous pouvez rencontrer l'un des problèmes suivants :

- Lorsque vous créez un Blueprint de clone lié, aucune machine ne s'affiche dans la liste à cloner ou la machine que vous souhaitez cloner ne s'affiche pas.
- Lorsque vous créez un Blueprint de clone, aucun modèle ne s'affiche dans la liste de modèles à cloner ou le modèle de votre choix ne s'affiche pas.

- Lorsque des machines sont demandées à l'aide de votre Blueprint de clone partagé, le provisionnement échoue.
- En raison de la chronologie de la collecte de données, un modèle ayant été supprimé est toujours visible pour les utilisateurs lorsqu'ils créent ou modifient des Blueprints de clone lié.

Cause

Plusieurs raisons peuvent expliquer les problèmes courants de Blueprint de clone et de clone lié.

Pour obtenir des informations connexes sur les options **Cloner à partir de** et **Cloner à partir d'un snapshot** avec **Utiliser le snapshot actuel** qui sont disponibles lorsque vous créez des Blueprints, reportez-vous à la section [Paramètres du composant de machine vSphere](#).

Tableau 3-30. Causes des problèmes courants de Blueprint de clone et de clone lié

Problème	Cause	Solution
Machines manquantes	Vous ne pouvez créer que des Blueprints de clones liés avec des machines que vous gérez en tant qu'administrateur de locataire ou gestionnaire de groupes d'activité.	Un utilisateur de votre locataire ou groupe d'activité doit demander une machine vSphere. Si vous disposez des rôles appropriés, vous pouvez le faire vous-même. Vous pouvez également afficher des machines non gérées dans cette boîte de dialogue. Les machines gérées peuvent avoir été importées. Les machines ne doivent pas obligatoirement avoir été provisionnées dans vRealize Automation pour s'afficher dans cette boîte de dialogue.
Modèles manquants	La collecte de données a échoué sur un point de terminaison donné ou aucun point de terminaison n'est disponible pour la plateforme du composant.	<ul style="list-style-type: none"> ■ Si vos points de terminaison sont en cluster et contiennent plusieurs ressources de calcul, vérifiez que votre administrateur IaaS a ajouté le cluster contenant les modèles à votre groupe Fabric. ■ Pour de nouveaux modèles, vérifiez que le service informatique a placé les modèles sur le même cluster inclus dans votre groupe Fabric.
Échec du provisionnement avec un Blueprint partagé	Pour les Blueprints, aucune validation ne permet de s'assurer que le modèle que vous avez sélectionné existe dans la réservation utilisée pour provisionner une machine à partir de votre Blueprint de clone partagé.	Envisagez d'utiliser des droits d'accès pour restreindre le Blueprint aux utilisateurs qui ont une réservation sur la ressource de calcul où le modèle existe.

Tableau 3-30. Causes des problèmes courants de Blueprint de clone et de clone lié (suite)

Problème	Cause	Solution
Échec du provisionnement avec un agent invité	Si la machine virtuelle redémarre immédiatement après la fin de la personnalisation du système d'exploitation invité, avant que les éléments de travail de l'agent invité soient terminés, cela entraîne l'échec du provisionnement. Vous pouvez utiliser la propriété personnalisée <code>VirtualMachine.Admin.CustomizeGuestOSDelay</code> pour augmenter le délai.	Vérifiez que vous avez ajouté la propriété personnalisée <code>VirtualMachine.Admin.CustomizeGuestOSDelay</code> . Cette valeur doit être dans le format HH:MM:SS. Si la propriété n'est pas définie, la valeur par défaut est une minute (00:01:00).
Le provisionnement de clone lié échoue lors de l'utilisation de SDRS	Lors de l'utilisation de provisionnement de clone lié et de SDRS, la nouvelle machine doit se trouver sur le même cluster. Une erreur de provisionnement se produit si les disques de la machine source se trouvent sur un cluster et que vous avez demandé de provisionner une machine sur un cluster différent.	Lors de l'utilisation de SDRS et de provisionnement de clone lié, provisionnez des machines situées sur le même cluster que la source du clone lié. Ne provisionnez pas sur un cluster différent.
Le provisionnement de Blueprint de clone ou de clone lié échoue, car il est impossible de trouver le modèle sur lequel le clone est basé.	Il n'est pas possible de provisionner des machines dans un Blueprint cloné à partir d'un modèle qui n'existe plus. vRealize Automation exécute régulièrement une collecte de données, par défaut toutes les 24 heures. Si un modèle est supprimé, la modification est visible à la prochaine collecte de données. Par conséquent, il est possible de créer un Blueprint basé sur un modèle inexistant.	Redéfinissez le Blueprint à l'aide d'un modèle existant, puis demandez le provisionnement. Par précaution et le cas échéant, vous pouvez exécuter une collecte de données avant de définir le Blueprint de clone ou de clone lié.

Conception de Blueprints avec des paramètres NSX

Si vous disposez d'une instance NSX intégrée à vRealize Automation, vous pouvez configurer vos Blueprints vSphere pour utiliser NSX à des fins de virtualisation de réseau et de sécurité.

Si vous avez configuré l'intégration de vRealize Automation à NSX, vous pouvez utiliser des composants réseau, de sécurité et d'équilibrage de charge dans le canevas de conception pour configurer votre Blueprint à des fins de provisionnement de machine. Vous pouvez également ajouter les paramètres réseau et de sécurité NSX suivants au Blueprint global, lorsque vous créez un Blueprint ou lorsque vous modifiez un Blueprint existant :

- Zone de transport : contient les réseaux utilisés pour le déploiement de la machine provisionnée.
- Stratégie de réservation de passerelle Edge et acheminée : gère la communication réseau pour le déploiement de la machine provisionnée.
- Isolation d'app : autorise uniquement le trafic interne entre les machines utilisées dans le déploiement de la machine provisionnée.

Pour plus d'informations sur l'intégration de vRealize Automation et de NSX, et l'utilisation des composants de réseau et de sécurité NSX dans le Blueprint vRealize Automation, reportez-vous à cet article de blog [vRA et NSX - Introduction à l'automatisation de mise en réseau et de sécurité](#).

Les paramètres NSX sont uniquement applicables à des types de composants de machine vSphere.

Paramètres de la page Nouveau Blueprint et Propriétés du Blueprint avec NSX

Vous pouvez spécifier des paramètres qui s'appliquent à l'intégralité du Blueprint, y compris certains paramètres NSX , à l'aide de la page **Nouveau Blueprint** lorsque vous créez le Blueprint. Après avoir créé le Blueprint, vous pouvez modifier ces paramètres dans la boîte de dialogue Propriétés du Blueprint.

Onglet Général

Appliquez des paramètres à votre Blueprint entier, y compris tous les composants que vous envisagez d'ajouter maintenant ou ultérieurement.

Tableau 3-31. Paramètres de l'onglet Général

Configuration	Description
Nom	Entrez le nom de votre Blueprint.
Identifiant	Le champ Identifiant est automatiquement renseigné avec le nom que vous avez entré. Vous pouvez modifier ce champ maintenant, mais une fois le Blueprint enregistré, vous ne pourrez plus le modifier. Du fait que les identifiants sont permanents et uniques au sein de votre locataire, vous pouvez les utiliser pour interagir par programmation avec les Blueprints et pour créer des liaisons de propriétés.
Description	Résumez votre Blueprint à l'attention d'autres architectes. Cette description apparaît également aux utilisateurs spécifiés sur le formulaire de demande.
Archiver (jours)	Vous pouvez spécifier une période d'archivage pour conserver les déploiements de manière temporaire plutôt que détruire les déploiements dès l'expiration de leur bail. Spécifiez 0 (par défaut) pour détruire le déploiement à l'expiration de son bail. La période d'archivage commence le jour d'expiration du bail. À l'expiration de la période d'archivage, le déploiement est détruit.
Limite de déploiement	Spécifiez le nombre maximal de déploiements qui peuvent être créés lorsque ce Blueprint est utilisé pour provisionner des machines.
Bail (jours) : minimum et maximum	Entrez une valeur minimale et une valeur maximale pour permettre aux utilisateurs de choisir parmi plusieurs durées de bail. Lorsque le bail se termine, le déploiement est détruit ou archivé. Si vous ne spécifiez pas de valeurs minimale et maximale, le bail devient perpétuel.

Onglet Paramètres NSX

Si vous avez configuré NSX, vous pouvez spécifier la zone de transport NSX, la stratégie de réservation de passerelle Edge et acheminée, et les paramètres d'isolation d'application lorsque vous créez ou modifiez un Blueprint. Ces paramètres sont disponibles dans l'onglet **Paramètres NSX** sur les pages **Blueprint** et **Propriétés du Blueprint**.

Pour plus d'informations sur la configuration de NSX, reportez-vous au *Guide d'administration de NSX*.

Tableau 3-32. Paramètres de l'onglet Paramètres NSX

Configuration	Description
Zone de transport	<p>Sélectionnez une zone de transport NSX existante pour contenir le ou les réseaux que le déploiement des machines provisionnées peut utiliser.</p> <p>Une zone de transport définit les clusters que les réseaux peuvent recouvrir. Lors du provisionnement de machines, si une zone de transport est spécifiée dans une réservation et un Blueprint, les valeurs de la zone de transport doivent correspondre.</p> <p>Une zone de transport est requise uniquement pour les Blueprints qui disposent d'un réseau à la demande. Pour les groupes de sécurité, les balises de sécurité et les équilibrages de charge, la zone de transport est facultative. Si vous ne spécifiez pas de zone de transport, le point de terminaison est déterminé par l'emplacement du groupe de sécurité, la balise de sécurité ou le réseau auquel l'équilibrage de charge se connecte.</p>
Stratégie de réservation de passerelle Edge et acheminée	<p>Sélectionnez une stratégie de réservation de passerelle acheminée NSX. Cette stratégie de réservation s'applique aux passerelles acheminées et à tous les dispositifs Edge qui sont déployés dans le cadre d'un provisionnement. Un seul périphérique Edge est provisionné par déploiement.</p> <p>Pour les réseaux acheminés, les périphériques Edge ne sont pas provisionnés, mais vous pouvez utiliser une stratégie de réservation afin de sélectionner une réservation avec les passerelles acheminées à utiliser pour le provisionnement des réseaux acheminés.</p> <p>Lorsque vRealize Automation provisionne une machine avec une mise en réseau NAT ou acheminée, il provisionne une passerelle acheminée comme routeur réseau. La passerelle Edge ou acheminée est une machine de gestion qui consomme des ressources de calcul telles que d'autres machines virtuelles mais gère les communications réseau avec toutes les machines de ce déploiement. La réservation utilisée pour provisionner la passerelle Edge ou acheminée détermine le réseau externe utilisé pour NAT et les adresses IP virtuelles de l'équilibrage de charge. Il est recommandé d'utiliser des clusters de gestion distincts pour les machines de gestion comme les dispositifs NSX Edge.</p>
Isolation d'app	<p>Sélectionnez la case à cocher Isolation d'app pour utiliser la stratégie de sécurité d'isolation d'application configurée dans NSX. La stratégie d'isolation d'application s'applique à tous les composants de la machine vSphere du Blueprint. Vous pouvez éventuellement ajouter des groupes de sécurité et des balises NSX pour permettre à vRealize Orchestrator d'ouvrir la configuration de réseau isolé afin d'autoriser des chemins d'accès supplémentaires vers l'isolation d'application et en provenance de celle-ci.</p>

Onglet Propriétés

Les propriétés personnalisées que vous ajoutez au niveau du Blueprint s'appliquent à l'intégralité du Blueprint, y compris l'ensemble de ses composants. Cependant, elles peuvent être remplacées par des propriétés personnalisées attribuées ultérieurement dans la chaîne de priorité. Pour plus d'informations sur l'ordre de priorité des propriétés personnalisées, reportez-vous à *Référence des propriétés personnalisées*.

Tableau 3-33. Paramètres de l'onglet Propriétés

Onglet	Configuration	Description
Groupes de propriétés		Les groupes de propriétés sont des groupes de propriétés réutilisables qui sont destinés à simplifier le processus d'ajout de propriétés personnalisées aux Blueprints. Vos gestionnaires de locataires et administrateurs Fabric peuvent regrouper les propriétés qui sont souvent utilisées ensemble de sorte que vous puissiez ajouter le groupe de propriétés à un Blueprint plutôt qu'insérer individuellement des propriétés personnalisées.
	Ajouter	<p>Ajoutez un ou plusieurs groupes de propriétés existants et appliquez-les au Blueprint global.</p> <p>Les groupes de propriétés liées à des conteneurs suivants sont fournis :</p> <ul style="list-style-type: none"> ■ Propriétés de l'hôte du conteneur avec authentification par certificat ■ Propriétés de l'hôte du conteneur avec authentification par utilisateur/mot de passe
	Monter /Descendre	Contrôlez l'ordre de priorité donné à chaque groupe de propriétés par rapport aux autres en classant les groupes par ordre de priorité. Le premier groupe de la liste a le niveau de priorité le plus élevé et ses propriétés personnalisées sont prioritaires. Vous pouvez également utiliser la fonction de glisser-déposer pour changer l'ordre.
	Afficher les propriétés	Affichez les propriétés personnalisées du groupe de propriétés sélectionné.
	Afficher les propriétés fusionnées	Si une propriété personnalisée est incluse dans plusieurs groupes de propriétés, la valeur incluse dans le groupe de propriétés avec le niveau de priorité le plus élevé est prioritaire. Vous pouvez afficher ces propriétés fusionnées pour vous aider à classer les groupes de propriétés par ordre de priorité.
Propriétés personnalisées		Vous pouvez ajouter des propriétés personnalisées individuelles au lieu des groupes de propriétés.
	Nouveau	Ajoutez une propriété personnalisée individuelle et appliquez-la au Blueprint global.
	Nom	Entrez le nom de la propriété. Pour obtenir la liste des propriétés personnalisées et leurs définitions, reportez-vous à <i>Référence des propriétés personnalisées</i> .
	Valeur	Entrez la valeur de la propriété personnalisée.

Tableau 3-33. Paramètres de l'onglet Propriétés (suite)

Onglet	Configuration	Description
	Chiffré	Vous pouvez choisir de chiffrer la valeur de la propriété, par exemple, si la valeur est un mot de passe.
	Remplaçable	Vous pouvez spécifier que la valeur de la propriété peut être remplacée par la prochaine personne qui utilise la propriété. Il s'agit généralement d'un autre architecte, mais si vous sélectionnez Afficher dans la demande, vos utilisateurs peuvent voir et modifier les valeurs des propriétés lorsqu'ils demandent des éléments du catalogue.
	Afficher dans la demande	Si vous souhaitez afficher le nom et la valeur de la propriété pour vos utilisateurs finaux, vous pouvez indiquer d'afficher la propriété sur le formulaire de demande lors de la demande de provisionnement de machine. Vous pouvez également sélectionner Remplaçable si vous souhaitez que les utilisateurs fournissent une valeur.

Application d'une zone de transport NSX à un Blueprint

Un administrateur NSX peut créer des zones de transport pour contrôler l'utilisation de cluster des réseaux.

Si le Blueprint contient un réseau à la demande, vous devez spécifier la zone de transport NSX qui contient les réseaux utilisés par le déploiement de la machine provisionnée. La même zone de transport doit être spécifiée dans la réservation.

Application d'une stratégie de réservation de passerelle Edge ou acheminée NSX à un Blueprint

Vous pouvez spécifier une stratégie de réservation pour gérer les communications réseau pour les machines provisionnées par le Blueprint. Lorsque le provisionnement des machines est demandé, la stratégie de réservation est utilisée pour regrouper les réservations qui peuvent être prises en compte pour le déploiement. La stratégie de réservation de passerelle acheminée est également appelée stratégie de réservation Edge.

Les informations de mise en réseau sont contenues dans chaque réservation. Lorsque les machines sont provisionnées, une passerelle Edge ou acheminée est allouée comme routeur réseau pour gérer les communications réseau pour les machines provisionnées dans le déploiement. Vous pouvez ajouter ou modifier des propriétés au niveau du Blueprint via la page des propriétés du Blueprint.

Une stratégie de réservation de passerelle acheminée est facultative. Elle contrôle la ou les réservations pouvant être utilisées pour provisionner NSX Edge associé à la mise en réseau à la demande et aux composants d'équilibrage de charge à la demande spécifiés dans le Blueprint.

Vous utilisez des stratégies de réservation pour contrôler la sélection des réservations. Vous sélectionnez une stratégie de réservation dans la définition des machines virtuelles du Blueprint et vous l'affectez aux réservations que vos machines virtuelles doivent utiliser.

Vous ne pouvez pas partager de réservations entre plusieurs groupes d'activité.

vRealize Automation provisionne une passerelle acheminée, par exemple une passerelle de services de périphérie (ESG) pour les réseaux NAT et les équilibres de charge. Pour les réseaux routés, vRealize Automation utilise les routeurs distribués existants.

Un profil réseau NAT et un équilibre de charge permettent à vRealize Automation de déployer une passerelle de services de périphérie NSX. Un profil réseau acheminé utilise un routeur distribué logique (DLR) NSX. Le DLR doit être créé dans NSX avant de pouvoir être utilisé par vRealize Automation. vRealize Automation ne peut pas créer de DLR. Après la collecte des données, vRealize Automation peut utiliser le DLR pour le provisionnement de machines virtuelles.

La réservation utilisée pour provisionner la passerelle Edge ou acheminée détermine le réseau externe utilisé pour les profils réseau NAT et acheminés, ainsi que les adresses IP virtuelles de l'équilibre de charge.

Lorsque vous utilisez le Blueprint pour provisionner un déploiement de machine, vRealize Automation tente d'utiliser uniquement les réservations associées à la stratégie de réservation spécifiée pour provisionner la passerelle Edge ou acheminée.

Application d'une stratégie de sécurité d'isolation d'app NSX à un Blueprint

Une stratégie d'isolation d'app NSX agit en tant que pare-feu pour bloquer tout le trafic entrant et sortant depuis et vers les machines provisionnées dans le déploiement. Lorsque vous spécifiez une stratégie d'isolation d'app NSX définie, les machines provisionnées par le Blueprint peuvent communiquer entre elles mais ne peuvent pas se connecter en dehors du pare-feu.

Vous pouvez appliquer une isolation d'application au niveau du Blueprint à l'aide de la page **Nouveau Blueprint** ou **Propriétés du Blueprint**.

Lorsque vous utilisez une stratégie d'isolation d'app NSX, seul le trafic interne entre les machines provisionnées par le Blueprint est autorisé. Lorsque vous demandez le provisionnement, un groupe de sécurité est créé pour les machines qui doivent être provisionnées. Une stratégie de sécurité d'isolation d'app est créée dans NSX et appliquée au groupe de sécurité. Des règles de pare-feu sont définies dans la stratégie de sécurité pour autoriser uniquement le trafic interne entre les composants qui figurent dans le déploiement. Pour des informations complémentaires, consultez [Créer un point de terminaison NSX et l'associer à un point de terminaison vSphere](#).

Remarque Lorsque le provisionnement est effectué avec un Blueprint qui utilise un équilibrage de charge Edge NSX et une stratégie de sécurité d'isolation d'app NSX, l'équilibrage de charge provisionné dynamiquement n'est pas ajouté au groupe de sécurité. Ceci empêche l'équilibrage de charge de communiquer avec les machines pour lesquelles il doit gérer des connexions. Du fait que les dispositifs Edge sont exclus du pare-feu distribué NSX, ils ne peuvent pas être ajoutés aux groupes de sécurité. Pour que l'équilibrage de charge fonctionne correctement, utilisez un autre groupe de sécurité ou une autre stratégie de sécurité qui autorise le trafic requis dans le composant de machines virtuelles pour l'équilibrage de charge.

La stratégie d'isolation d'app a un ordre de priorité moins élevé que les autres stratégies de sécurité dans NSX. Par exemple, si le déploiement des machines provisionnées contient une machine de composant Web et une machine de composant App et que la machine du composant Web héberge un service Web, le service doit alors autoriser le trafic entrant sur les ports 80 et 443. Dans ce cas, les utilisateurs doivent créer une stratégie de sécurité Web dans NSX avec les règles de pare-feu définies pour autoriser le trafic entrant sur ces ports. Dans vRealize Automation, les utilisateurs doivent appliquer la stratégie de sécurité Web sur le composant Web du déploiement des machines provisionnées.

Remarque Si un Blueprint contient un ou plusieurs équilibres de charge et que l'isolation d'application est activée pour le Blueprint, l'équilibrage de charge, les adresses IP virtuelles sont ajoutées au groupe de sécurité de l'isolation d'application comme IPSet. Si un Blueprint contient un groupe de sécurité à la demande qui est associé à un niveau de machine qui est également associé à un équilibrage de charge, le groupe de sécurité à la demande inclut le niveau de la machine et l'IPSet avec l'adresse IP virtuelle de l'équilibrage de charge.

Si la machine du composant Web doit accéder à la machine du composant App en utilisant un équilibrage de charge sur les ports 8080 et 8443, la stratégie de sécurité Web doit inclure également des règles de pare-feu pour autoriser le trafic sortant sur ces ports en plus des règles de pare-feu existantes qui autorisent le trafic entrant sur les ports 80 et 443.

Pour obtenir des informations complémentaires sur les fonctionnalités de sécurité qui peuvent être appliquées à un composant de machine dans un Blueprint, reportez-vous à [Utilisation de composants de sécurité dans le canevas de conception](#)

Configuration des paramètres de composants de réseau et de sécurité

vRealize Automation prend en charge les réseaux virtualisés basés sur la plate-forme NSX. Les réseaux Conteneurs pour vRealize Automation intégrés sont également pris en charge.

Pour intégrer le réseau et la sécurité à vRealize Automation, un administrateur IaaS doit configurer des points de terminaison vSphere et NSX.

Pour plus d'informations sur la préparation externe, reportez-vous à *Configuration de vRealize Automation*.

Vous pouvez créer des profils réseau qui spécifient les paramètres réseau dans les réservations et dans le canevas de conception. Les profils réseau externes définissent les réseaux physiques existants. Les profils NAT et acheminés sont des modèles utilisés pour créer des commutateurs NSX logiques et les paramètres de routage appropriés à un nouveau chemin réseau pour configurer des interfaces réseau permettant de se connecter au chemin réseau lors du provisionnement des machines virtuelles et de la configuration des dispositifs NSX Edge.

Les paramètres du composant réseau et de sécurité que vous ajoutez au canevas de conception proviennent de votre configuration NSX et nécessitent l'exécution d'une collecte de données pour l'inventaire NSX pour les clusters vSphere. Les composants réseau et sécurité sont spécifiques à NSX et sont disponibles pour être utilisés avec des composants de machine vSphere uniquement. Pour plus d'informations sur la configuration de NSX, reportez-vous au *Guide d'administration de NSX*.

Pour les composants de machine ne disposant pas d'un onglet **Réseau** ou **Sécurité**, vous pouvez ajouter des propriétés personnalisées réseau et de sécurité telles que `VirtualMachine.Network0.Name` à leur onglet **Propriétés** dans le canevas de conception. Les propriétés de réseau, de sécurité et d'équilibrage de charge NSX s'appliquent uniquement aux machines vSphere.

Si vous spécifiez un profil réseau dans une réservation et un Blueprint, la valeur du Blueprint est prioritaire. Par exemple, si vous spécifiez un profil réseau dans le Blueprint à l'aide de la propriété personnalisée `VirtualMachine.NetworkN.ProfileName` et dans une réservation utilisée par le Blueprint, le profil réseau spécifié dans le Blueprint est prioritaire. Toutefois, si la propriété personnalisée n'est pas utilisée dans le Blueprint et que vous sélectionnez un profil réseau pour la carte réseau d'une machine, vRealize Automation utilise le chemin d'accès de réseau de réservation pour la carte réseau de la machine pour laquelle le profil réseau est spécifié.

En fonction de la ressource de calcul, vous pouvez sélectionner une zone de transport qui identifie un point de terminaison vSphere. Une zone de transport spécifie les hôtes et les clusters qui peuvent être associés aux commutateurs logiques créés dans la zone. Une zone de transport peut couvrir plusieurs clusters vSphere. Le Blueprint et les réservations utilisés dans le provisionnement doivent avoir les mêmes paramètres de zone de transport. Les zones de transport sont définies dans les environnements NSX. Reportez-vous au *Guide d'administration de NSX*.

Vous pouvez configurer des paramètres de sécurité pour les machines virtuelles à provisionner en spécifiant des informations dans un script de réservation, de Blueprint ou d'agent invité. Si les machines à provisionner nécessitent un agent invité, vous devez ajouter une règle de sécurité contenant cette exigence à la réservation ou au Blueprint. Par exemple, si vous utilisez une stratégie de sécurité par défaut qui refuse la communication entre toutes les machines, et vous fiez à une stratégie de sécurité distincte

qui autorise la communication entre des machines spécifiques, l'agent invité doit être en mesure de communiquer avec vRealize Automation pendant la phase de personnalisation. Pour éviter ce problème lors du provisionnement des machines, utilisez une stratégie de sécurité par défaut qui autorise la communication pendant la phase de personnalisation.

Vous pouvez également ajouter un composant réseau Conteneurs à un Blueprint.

Utilisation de composants réseau dans le canevas de conception

Vous pouvez ajouter un ou plusieurs composants réseau NSX au canevas de conception et configurer leurs paramètres pour les composants de machine vSphere dans le Blueprint.

Vous pouvez ajouter des composants réseau au canevas de conception pour rendre leurs paramètres configurés disponibles pour un ou plusieurs composants de machine dans le Blueprint.

Les paramètres du composant réseau et de sécurité que vous ajoutez au canevas de conception proviennent de votre configuration NSX et nécessitent l'exécution d'une collecte de données pour l'inventaire NSX pour les clusters vSphere. Les composants réseau et sécurité sont spécifiques à NSX et sont disponibles pour être utilisés avec des composants de machine vSphere uniquement. Pour plus d'informations sur la configuration de NSX, reportez-vous au *Guide d'administration de NSX*.

Ajouter un composant réseau existant

Vous pouvez ajouter un composant réseau NSX existant au canevas de conception lors de la préparation de l'association de ses paramètres à un ou plusieurs composants de machine vSphere du Blueprint.

Vous pouvez utiliser un composant réseau existant pour ajouter un réseau NSX au canevas de conception et configurer ses paramètres à utiliser avec les composants de machine vSphere et les composants Logiciel ou XaaS qui concernent vSphere.

Lorsque vous associez un composant existant ou un composant réseau à la demande à un composant de machine, les informations de la carte réseau sont stockées avec le composant de la machine. Les informations sur le profil réseau que vous spécifiez sont stockées avec le composant réseau.

Vous pouvez ajouter plusieurs composants réseau et de sécurité au canevas de conception.

Pour les composants de machine ne disposant pas d'un onglet **Réseau** ou **Sécurité**, vous pouvez ajouter des propriétés personnalisées réseau et de sécurité telles que `VirtualMachine.Network0.Name` à leur onglet **Propriétés** dans le canevas de conception. Les propriétés de réseau, de sécurité et d'équilibrage de charge NSX s'appliquent uniquement aux machines vSphere.

Prérequis

- Créez et configurez des paramètres réseau pour NSX. Reportez-vous à la section *Configuration de vRealize Automation* et au *Guide d'administration de NSX*.
- Vérifiez que l'inventaire NSX a été exécuté avec succès pour votre cluster.
Pour utiliser des configurations NSX dans vRealize Automation, vous devez exécuter la collecte de données.
- Créez un profil réseau.
- Connectez-vous à la console vRealize Automation en tant qu'**architecte d'infrastructure**.

- Ouvrez un nouveau Blueprint ou un Blueprint existant dans le canevas de conception via l'onglet **Conception**.

Procédure

- 1 Cliquez sur **Réseau et sécurité** dans la section Catégories pour afficher la liste des composants réseau et de sécurité disponibles.

- 2 Faites glisser un composant de **Réseau existant** vers le canevas de conception.

- 3 Cliquez dans la zone de texte **Réseau existant** et sélectionnez un profil de réseau existant.

La description, les valeurs de masque de sous-réseau et de passerelle sont renseignées sur la base du profil réseau sélectionné.

- 4 (Facultatif) Cliquez sur l'onglet **DNS/WINS**.

- 5 (Facultatif) Spécifiez ou acceptez les paramètres DNS et WINS du profil réseau.

- DNS principal
- DNS secondaire
- Suffixe DNS
- Serveur WINS préféré
- Serveur WINS auxiliaire

Vous ne pouvez pas modifier les paramètres DNS ou WINS pour un réseau existant.

- 6 (Facultatif) Cliquez sur l'onglet **Plages d'adresses IP**.

La ou les plages d'adresses IP spécifiées dans le profil réseau s'affichent. Vous pouvez modifier l'ordre de tri ou l'affichage de la colonne. Pour les réseaux NAT, vous pouvez également modifier les valeurs de plage IP.

- 7 Cliquez sur **Terminer** pour enregistrer le Blueprint en tant que brouillon ou poursuivez la configuration du Blueprint.

Suivant

Vous pouvez continuer à configurer des paramètres réseau en ajoutant des composants de sécurité supplémentaires et en sélectionnant des paramètres dans l'onglet **Réseau** d'un composant de machine vSphere dans le canevas de conception.

Création et utilisation de règles NAT

Vous pouvez ajouter des règles NAT à un composant réseau NAT Un à plusieurs dans un Blueprint lorsque le composant réseau NAT est associé à un composant de machine vSphere non ordonné en cluster ou un composant d'équilibrage de charge NSX à la demande.

Vous pouvez définir des règles NAT pour n'importe quel protocole pris en charge par NSX. Vous pouvez mapper un port ou une plage de ports à partir de l'adresse IP externe d'un dispositif Edge à une adresse IP privée dans le composant réseau NAT.

- Composants de machines vSphere

Vous pouvez créer des règles NAT pour un composant réseau Un à plusieurs NAT qui est associé à un composant de machine vSphere non ordonné en cluster.

Par exemple, si deux machines sont associées à un composant réseau NAT Un à plusieurs sur le Blueprint, vous pouvez définir une règle NAT qui autorise le port 443 sur l'adresse IP externe à se connecter aux machines via le port 80 sur le réseau NAT à l'aide du protocole TCP.

- Composant d'équilibrage de charge NSX

Vous pouvez créer des règles NAT pour un composant réseau Un à plusieurs NAT qui est associé au réseau VIP d'un composant d'équilibrage de charge NSX.

Par exemple, si deux machines sont associées à un composant réseau NAT Un à plusieurs sur le Blueprint, vous pouvez définir une règle NAT qui autorise le port 90 sur l'adresse IP externe à se connecter aux machines via le port 80 sur le réseau NAT à l'aide du protocole TCP.

Vous pouvez créer un nombre quelconque de règles NAT et vous pouvez contrôler l'ordre dans lequel les règles sont traitées.

Les éléments suivants ne sont pas pris en charge pour les règles de NAT :

- Les cartes réseau qui ne sont pas dans le réseau actuel
- Les cartes réseau qui sont configurées pour obtenir les adresses IP à l'aide de DHCP
- Les clusters de machines

Pour ajouter des règles NAT à un composant réseau NAT dans un Blueprint, reportez-vous à la section [Ajouter un composant réseau NAT à la demande ou routé à la demande](#).

Pour obtenir des informations connexes sur l'utilisation des règles NAT, consultez les articles publics tels que ce [billet de blog vmwarelab](#).

Ajouter un composant réseau NAT à la demande ou routé à la demande

Vous pouvez ajouter un composant réseau NSX NAT à la demande ou un composant réseau NSXrouté à la demande au canevas de conception lors de la préparation de l'association de leurs paramètres à un ou plusieurs composants de machine vSphere dans le Blueprint.

Lorsque vous associez un composant existant ou un composant réseau à la demande à un composant de machine, les informations de la carte réseau sont stockées avec le composant de la machine. Les informations sur le profil réseau que vous spécifiez sont stockées avec le composant réseau.

Vous pouvez ajouter plusieurs composants réseau et de sécurité au canevas de conception.

Un Blueprint peut inclure plusieurs composants de réseau à la demande. Cependant, tous les profils réseau à la demande qui sont utilisés dans le Blueprint doivent faire référence au même profil réseau externe.

Pour les composants de machine ne disposant pas d'un onglet **Réseau** ou **Sécurité**, vous pouvez ajouter des propriétés personnalisées réseau et de sécurité telles que `VirtualMachine.Network0.Name` à leur onglet **Propriétés** dans le canevas de conception. Les propriétés de réseau, de sécurité et d'équilibrage de charge NSX s'appliquent uniquement aux machines vSphere.

Prérequis

- Créez et configurez des paramètres réseau pour NSX. Reportez-vous à la section *Configuration de vRealize Automation* et au Guide d'administration de NSX.
- Vérifiez que l'inventaire NSX a été exécuté avec succès pour votre cluster.
Pour utiliser des configurations NSX dans vRealize Automation, vous devez exécuter la collecte de données.
- Créez un profil réseau à la demande. Reportez-vous à [Création d'un profil réseau](#).
Par exemple, si vous ajoutez un composant réseau NAT à la demande, reportez-vous à [Création d'un profil réseau NAT pour un réseau à la demande](#).
- Connectez-vous à la console vRealize Automation en tant qu'**architecte d'infrastructure**.
- Ouvrez un nouveau Blueprint ou un Blueprint existant dans le canevas de conception via l'onglet **Conception**.
- Si vous voulez spécifier des règles NAT pour un composant réseau NAT, vous devez utiliser un profil réseau NAT un-à-plusieurs. Reportez-vous à [Créer un profil réseau NAT en utilisant le point de terminaison IPAM fourni](#) ou [Créer un profil de réseau NAT au moyen d'un point de terminaison IPAM tiers](#). Pour plus d'informations sur les règles NAT, reportez-vous à la section [Création et utilisation de règles NAT](#).

Procédure

- 1 Cliquez sur **Réseau et sécurité** dans la section Catégories pour afficher la liste des composants réseau et de sécurité disponibles.
- 2 Faites glisser un réseau NAT à la demande ou un composant réseau acheminé à la demande vers le canevas de conception.
- 3 Entrez un nom de composant dans la zone de texte **ID**, afin d'attribuer une étiquette unique au composant dans le canevas de conception.
- 4 Sélectionnez un profil réseau approprié dans le menu déroulant **Profil réseau parent**. Par exemple, si vous souhaitez ajouter un composant réseau NAT, sélectionnez un profil réseau NAT configuré pour prendre en charge vos paramètres réseau.

Si vous voulez spécifier des règles NAT dans un composant réseau NAT, vous devez utiliser un profil réseau parent configuré pour un réseau NAT un-à-plusieurs.

Selon le type de profil sélectionné, les paramètres réseau suivants sont renseignés en fonction du profil réseau sélectionné. Les modifications de ces valeurs doivent être effectuées dans le profil réseau :

- Nom du profil réseau externe
- Type NAT (réseau NAT à la demande)
- Masque de sous-réseau
- Masque de sous-réseau de la plage (réseau acheminé à la demande)

- Masque de sous-réseau de la plage (réseau acheminé à la demande)
- Adresse IP de base (réseau routé à la demande)

5 (Facultatif) Entrez une description du composant dans la zone de texte **Description**.

6 (Facultatif) Cliquez sur l'onglet **DNS/WINS**.

7 (Facultatif) Spécifiez ou acceptez les paramètres DNS et WINS du profil réseau.

- DNS principal
- DNS secondaire
- Suffixe DNS
- Serveur WINS préféré
- Serveur WINS auxiliaire

Vous ne pouvez pas modifier les paramètres DNS ou WINS pour un réseau existant.

8 Cliquez sur l'onglet **Plages d'adresses IP**.

La ou les plages d'adresses IP spécifiées dans le profil réseau s'affichent. Vous pouvez modifier l'ordre de tri ou l'affichage de la colonne. Pour les réseaux NAT, vous pouvez également modifier les valeurs de plage IP.

- a Entrez une valeur d'adresse IP de début dans la zone de texte **Début de la plage d'adresses IP**.
- b Entrez une valeur d'adresse IP de début dans la zone de texte **Début de la plage d'adresses IP**.

9 Si vous utilisez un réseau NAT basé sur un profil réseau NAT un-à-plusieurs qui utilise des plages d'adresses IP statiques, vous pouvez utiliser l'onglet **Règles NAT** pour ajouter des règles permettant à une adresse IP externe d'accéder aux composants dans le réseau NAT interne.

Pour un réseau Un à plusieurs NAT, vous pouvez définir les règles NAT qui peuvent être configurées lors de l'ajout d'un composant réseau NAT au Blueprint et être modifiés lorsque vous modifiez le réseau NAT dans un déploiement.

Les options disponibles sont basées sur les composants de machine vSphere ou d'équilibrage de charge NSX que vous avez associés au composant réseau NAT.

- **Nom** : entrez un nom de règle unique.
- **Composant** : sélectionnez un composant dans la liste des composants de machine ou d'équilibrage de charge vSphere associés au réseau NAT.
- **Port source** : sélectionnez l'option ANY, entrez un port ou une plage de ports valide ou spécifiez une liaison de propriétés valide.
- **Port de destination** : sélectionnez l'option ANY, entrez un port ou une plage de ports valide ou spécifiez une liaison de propriétés valide.
- **Protocole** : entrez n'importe quel protocole valide pris en charge par NSX ou sélectionnez l'option TCP, UDP ou ANY.
- **Description** : entrez une brève description de l'utilisation de la règle NAT.

- 10** Cliquez sur **Terminer** pour enregistrer le Blueprint en tant que brouillon ou poursuivez la configuration du Blueprint.

Suivant

Vous pouvez continuer à configurer des paramètres réseau en ajoutant des composants de sécurité supplémentaires et en sélectionnant des paramètres dans l'onglet **Réseau** d'un composant de machine vSphere dans le canevas de conception.

Utilisation de composants d'équilibrage de charge dans le canevas de conception

Vous pouvez ajouter un ou plusieurs composants d'équilibrage de charge NSX à la demande aux canevas de conception pour configurer les paramètres du composant de machine vSphere dans le Blueprint.

Les paramètres du composant réseau et de sécurité que vous ajoutez au canevas de conception proviennent de votre configuration NSX et nécessitent l'exécution d'une collecte de données pour l'inventaire NSX pour les clusters vSphere. Les composants réseau et sécurité sont spécifiques à NSX et sont disponibles pour être utilisés avec des composants de machine vSphere uniquement. Pour plus d'informations sur la configuration de NSX, reportez-vous au *Guide d'administration de NSX*.

Les règles suivantes s'appliquent aux pools d'équilibrages de charge et aux paramètres réseau VIP du Blueprint.

- Si le profil réseau du pool est NAT, le profil réseau VIP peut faire partie du profil réseau NAT.
- Si le profil réseau de pool est routé, le profil réseau VIP ne peut être que sur le même réseau routé.
- Si le profil réseau de pool est externe, le profil réseau VIP ne peut être que le même profil réseau externe.

Chaque composant d'équilibrage de charge peut avoir plusieurs serveurs virtuels, qui sont également appelés services d'équilibrage de charge. Chaque serveur virtuel du composant d'équilibrage de charge dispose d'un port et d'un protocole. Par exemple, vous pouvez appliquer l'équilibrage de charge à un service HTTP ou à un service HTTPS. Un équilibrage de charge peut gérer plusieurs services dont il équilibre la charge.

Le dispositif Edge NSX est le périphérique réseau contenant les serveurs virtuels de l'équilibrage de charge. Vous pouvez disposer de plus d'un composant d'équilibrage de charge dans un Blueprint, lorsque vous provisionnez le déploiement, les serveurs virtuels définis dans chaque composant d'équilibrage de charge sont contenus dans un seul dispositif Edge NSX.

Si un Blueprint contient un ou plusieurs équilibrages de charge et que l'isolation d'application est activée pour le Blueprint, l'équilibrage de charge, les adresses IP virtuelles sont ajoutées au groupe de sécurité de l'isolation d'application comme IPSet. Si un Blueprint contient un groupe de sécurité à la demande qui est associé à un niveau de machine qui est également associé à un équilibrage de charge, le groupe de sécurité à la demande inclut le niveau de la machine et l'IPSet avec l'adresse IP virtuelle de l'équilibrage de charge.

Vous pouvez reconfigurer les paramètres d'équilibrage de charge dans un déploiement existant pour ajouter, modifier ou supprimer des serveurs virtuels. Pour plus d'informations, reportez-vous à [Reconfigurer un équilibrage de charge dans un déploiement](#).

Pour plus d'informations sur l'utilisation de composants d'équilibrage de charge après la mise à niveau ou la migration, reportez-vous à la section [Considérations lors de l'utilisation de composants d'équilibrage de charge mis à niveau ou migrés](#).

Considérations lors de l'utilisation de composants d'équilibrage de charge mis à niveau ou migrés

Les considérations suivantes sont importantes pour comprendre et prendre des mesures sur les composants d'équilibrage de charge NSX de la version de vRealize Automation cible.

Ces informations s'appliquent aux composants d'équilibrage de charge NSX qui ont été mis à niveau ou migrés vers cette version de vRealize Automation.

- Vous devez exécuter la collecte des données d'inventaire réseau et sécurité NSX avant et après la mise à niveau ou la migration vers cette version afin d'éviter des problèmes lors de l'exécution de l'action Reconfigurer l'équilibrage de charge. L'action Reconfigurer l'équilibrage de charge pour les nouveaux déploiements n'est pas affectée.

Pour plus d'informations, reportez-vous aux sections *Mise à niveau de vRealize Automation 7.1 ou 7.2 vers la version 7.3* et *Migration de vRealize Automation vers la version 7.3*.

- À compter de vRealize Automation 7.3, vous pouvez reconfigurer un équilibrage de charge. Le droit d'accès de catalogue requis est Reconfigurer (Équilibrage de charge). Pour des informations complémentaires, reportez-vous à [Reconfigurer un équilibrage de charge dans un déploiement](#).
- Pour les déploiements mis à niveau ou migrés de vRealize Automation 7.x vers cette version de vRealize Automation, la reconfiguration de l'équilibrage de charge est limitée aux déploiements qui contiennent un équilibrage de charge unique.
- L'opération Reconfigurer l'équilibrage de charge n'est pas prise en charge pour les déploiements mis à niveau ou migrés depuis vRealize Automation 6.2.x vers cette version vRealize Automation.

Ajouter un composant d'équilibrage de charge à la demande

Vous pouvez déplacer un composant d'équilibrage de charge à la demande NSX sur le canevas de conception et configurer ses paramètres pour une utilisation avec des composants de machine vSphere et des composants de conteneur dans le Blueprint.

Pour obtenir des informations connexes sur la création de profils d'application NSX pour définir le comportement d'un type de trafic réseau particulier, reportez-vous au *Guide d'administration de NSX* de votre version à l'adresse https://www.vmware.com/support/pubs/nsx_pubs.html.

Procédure

1 Définir les paramètres d'un membre d'équilibrage de charge

Vous pouvez définir un composant d'équilibrage de charge NSX à la demande pour distribuer le traitement des tâches entre les machines membres ou machines conteneurs vSphere provisionnées dans un réseau.

2 Définir les paramètres généraux du serveur virtuel

Vous pouvez définir un protocole et un port de serveur virtuel unique pour votre équilibrage de charge ou vous pouvez ajouter des serveurs virtuels supplémentaires pour personnaliser des options d'équilibrage de charge NSX supplémentaires.

3 Définir les paramètres de distribution de serveur virtuel

En sélectionnant l'option **Personnaliser** de l'onglet **Général**, vous pouvez spécifier des informations sur les membres du pool (comme le port sur lequel les membres reçoivent le trafic, le type de protocole que l'équilibrage de charge NSX peut utiliser pour accéder à ce port, l'algorithme utilisé pour l'équilibrage de charge et les paramètres de persistance).

4 Définir les paramètres de vérification de santé d'un serveur virtuel

En sélectionnant l'option **Personnaliser** dans l'onglet **Général**, vous pouvez spécifier comment, ou dans quelles circonstances, l'équilibrage de charge NSX effectue des contrôles de santé sur les membres du pool dans le serveur virtuel.

5 Définir les paramètres avancés de serveur virtuel

Lorsque vous sélectionnez l'option **Personnaliser** de l'onglet **Général**, vous pouvez personnaliser le composant d'équilibrage de charge NSX pour spécifier des paramètres tels que le nombre de connexions simultanées qu'un membre de pool unique peut reconnaître et le nombre maximal de connexions simultanées que le serveur virtuel peut traiter.

6 Définir les options de journalisation d'équilibrage de charge

Vous pouvez définir les types d'actions de journalisation d'équilibrage de charge qui sont capturées et enregistrées dans les journaux d'équilibrage de charge.

Définir les paramètres d'un membre d'équilibrage de charge

Vous pouvez définir un composant d'équilibrage de charge NSX à la demande pour distribuer le traitement des tâches entre les machines membres ou machines conteneurs vSphere provisionnées dans un réseau.

Lorsque vous ajoutez un composant d'équilibrage de charge à un Blueprint dans le canevas de conception, vous pouvez choisir une option par défaut ou personnalisée lors de la création ou de la modification des définitions de votre serveur virtuel dans le composant d'équilibrage de charge. L'option par défaut vous permet de spécifier le protocole, le port et la description du serveur virtuel, et d'utiliser les valeurs par défaut pour tous les autres paramètres. L'option personnalisée vous permet de définir des niveaux de détail supplémentaires.

Si l'équilibrage de charge est provisionné avec un réseau externe, l'adresse IP virtuelle (spécifiée avec **Réseau VIP**) et le pool de membre (spécifié avec **Réseau membre**) doivent se trouver sur le même réseau existant. Si l'adresse IP virtuelle et le pool ne sont pas sur le même réseau externe, une erreur se produit lors du provisionnement.

Prérequis

- Créez et configurez des paramètres d'équilibrage de charge pour NSX. Reportez-vous à la section *Configuration de vRealize Automation* et au Guide d'administration de NSX.

- Vérifiez que l'inventaire NSX a été exécuté avec succès pour votre cluster.

Pour utiliser des configurations NSX dans vRealize Automation, vous devez exécuter la collecte de données.

- Créez un profil réseau.
- Connectez-vous à la console vRealize Automation en tant qu'**architecte d'infrastructure**.
- Ouvrez un nouveau Blueprint ou un Blueprint existant dans le canevas de conception via l'onglet **Conception**.
- Vérifiez que le Blueprint comporte au moins un composant de machine vSphere ou un composant de conteneur.

Procédure

- 1 Cliquez sur **Réseau et sécurité** dans la section Catégories pour afficher la liste des composants réseau et de sécurité disponibles.
- 2 Faites glisser un composant d'**Équilibrage de charge à la demande** vers le canevas de conception.
- 3 Entrez un nom de composant dans la zone de texte **ID**, afin d'attribuer une étiquette unique au composant dans le canevas de conception.
- 4 Sélectionnez un nom de composant de machine vSphere ou de composant de conteneur dans le menu déroulant **Membre**.

La liste contient uniquement les composants de machine et les composants de conteneur vSphere dans le Blueprint actif.

- 5 Sélectionnez la carte réseau devant faire l'objet d'un équilibrage de charge dans le menu déroulant **Réseau membre**.

La liste contient les cartes réseau qui sont définies pour le membre sélectionné de la machine vSphere.

- 6 Sélectionnez un réseau d'adresse IP virtuel disponible dans le menu déroulant **Réseau VIP**. Par exemple, sélectionnez un réseau NAT ou externe disponible.

Vous pouvez avoir plusieurs équilibrages de charge NSX et composants réseau NSX à la demande dans un blueprint, qui doivent tous être associés au même réseau VIP.

- 7 (Facultatif) Entrez une adresse IP valide pour la carte réseau dans la zone de texte **Adresse IP**.

Le paramètre par défaut est l'adresse IP statique associée au réseau VIP. Vous pouvez spécifier une autre adresse IP ou une plage d'adresses IP. Par défaut, l'adresse IP disponible suivante est allouée à partir du réseau VIP associé.

Laissez le champ Adresse IP vide pour allouer l'adresse IP à partir du réseau VIP associé pendant le provisionnement.

Vous ne pouvez spécifier d'adresse IP que lorsque le VIP est créé sur un réseau NAT.

- 8 Pour créer une définition de serveur virtuel, cliquez sur **Nouveau**, reportez-vous à la section [Définir les paramètres généraux du serveur virtuel](#).

Chaque composant d'équilibrage de charge nécessite au moins un serveur virtuel.

Pour spécifier des options de journalisation, reportez-vous à la section [Définir les options de journalisation d'équilibrage de charge](#).

Définir les paramètres généraux du serveur virtuel

Vous pouvez définir un protocole et un port de serveur virtuel unique pour votre équilibrage de charge ou vous pouvez ajouter des serveurs virtuels supplémentaires pour personnaliser des options d'équilibrage de charge NSX supplémentaires.

Par exemple, vous pouvez personnaliser le composant d'équilibrage de charge afin de définir des paramètres tels que le protocole et le port de contrôle de santé, l'algorithme, la persistance et la transparence.

Prérequis

[Définir les paramètres d'un membre d'équilibrage de charge](#).

Procédure

- 1 Cliquez sur l'onglet **Général** sur la page **Nouveau serveur virtuel**.
- 2 Sélectionnez le protocole de trafic réseau dans le menu déroulant **Protocole** à utiliser pour l'équilibrage de charge du serveur virtuel.

Les options de protocole sont HTTP, HTTPS, TCP et UDP.

- 3 Entrez une valeur de port dans la zone de texte **Port**.

Le protocole sélectionné détermine le paramètre de port par défaut.

Protocole	Port par défaut
HTTP	80
HTTPS	443
TCP	8080
UDP	aucune valeur par défaut

Les protocoles HTTP, HTTPS et TCP peuvent partager un port avec le protocole UDP. Par exemple, si le service 1 utilise TCP, HTTP ou HTTPS sur le port 80, le service 2 peut utiliser UDP sur le port 80. Si le service 1 utilise UDP sur le port 80, le service 2 ne peut pas utiliser UDP sur ce port.

- 4 (Facultatif) Entrez une description pour le composant du serveur virtuel.
- 5 Sélectionnez l'une des options de **Paramètres**.

■ Utiliser la valeur par défaut pour tous les autres paramètres

Acceptez tous les autres paramètres par défaut. Cliquez sur **OK** pour terminer la définition du composant d'équilibrage de charge et continuer à travailler dans le Blueprint.

Vous pouvez afficher les valeurs par défaut en cliquant sur **Personnaliser** et en examinant les autres options de l'onglet. Si les paramètres par défaut sont acceptables, cliquez sur **Utiliser la valeur par défaut pour tous les autres paramètres** dans l'onglet **Général**.

■ Personnaliser

Configurez le composant d'équilibrage de charge avec les paramètres supplémentaires, par exemple pour définir un autre protocole pour le contrôle de santé ou un autre port pour la surveillance du trafic de membres.

D'autres onglets s'affichent qui vous permettent d'ajouter des paramètres personnalisés.

Si vous avez sélectionné **Utiliser la valeur par défaut pour tous les autres paramètres** et que vous avez cliqué sur **OK**, vous avez terminé et vous pouvez continuer à définir ou modifier votre Blueprint dans le canevas de conception. Si vous avez sélectionné **Personnaliser**, passez à l'étape suivante.

- 6 Cliquez sur l'onglet **Distribution** et passez à la rubrique [Définir les paramètres de distribution de serveur virtuel](#) pour continuer à définir le serveur virtuel dans le composant d'équilibrage de charge NSX.

Définir les paramètres de distribution de serveur virtuel

En sélectionnant l'option **Personnaliser** de l'onglet **Général**, vous pouvez spécifier des informations sur les membres du pool (comme le port sur lequel les membres reçoivent le trafic, le type de protocole que l'équilibrage de charge NSX peut utiliser pour accéder à ce port, l'algorithme utilisé pour l'équilibrage de charge et les paramètres de persistance).

Un pool représente un cluster de machines faisant l'objet d'un équilibrage de charge. Un membre du pool correspond à une machine de ce cluster.

Les paramètres par défaut de protocole du membre et de port du membre correspondent aux paramètres de protocole et de port de la page **Général**.

Le pool de machines membres est affiché dans la valeur de l'option **Membre** de l'interface utilisateur du composant d'équilibrage de charge du Blueprint. L'entrée **Membre** est définie sur le pool ou sur un cluster de machines.

Prérequis

[Définir les paramètres généraux du serveur virtuel.](#)

Procédure

- 1 (Facultatif) Le paramètre **Protocole du membre** correspond au protocole que vous avez spécifié dans l'onglet **Général**. Ce paramètre définit comment le membre du pool doit recevoir le trafic réseau.
- 2 (Facultatif) Entrez un numéro de port dans la zone de texte **Port du membre** pour spécifier le port sur lequel le membre du pool doit recevoir le trafic réseau.

Par exemple, si la demande entrante sur l'adresse IP virtuelle (VIP) de l'équilibrage de charge est effectuée sur le port 80, vous voudrez éventuellement acheminer la demande vers un autre port, par exemple le port 8080, sur les membres du pool.

3 (Facultatif) Sélectionnez la méthode d'équilibrage d'algorithme pour ce pool.

Les options d'algorithme et les paramètres d'algorithme des options qui les nécessitent sont décrits dans le tableau suivant.

Option	Description et paramètres d'algorithme
ROUND_ROBIN	<p>Chaque serveur est utilisé à tour de rôle selon le poids qui lui est attribué.</p> <p>Si l'équilibrage de charge a été créé dans vRealize Automation, le poids est le même pour tous les membres.</p> <p>Il s'agit de l'algorithme le plus homogène et le plus équitable lorsque le temps de traitement du serveur continue à être réparti de manière égale.</p> <p>Les paramètres d'algorithme sont désactivés pour cette option.</p>
IP-HASH	<p>Sélectionne un serveur en fonction d'un hachage de l'adresse IP source et du poids total des serveurs en cours d'exécution.</p> <p>Les paramètres d'algorithme sont désactivés pour cette option.</p>
LEASTCONN	<p>Répartit les requêtes client sur plusieurs serveurs en se basant sur le nombre de connexions déjà sur le serveur.</p> <p>Les nouvelles connexions sont envoyées au serveur ayant le moins de connexions.</p> <p>Les paramètres d'algorithme sont désactivés pour cette option.</p>
URI	<p>La partie gauche de l'URI (avant le point d'interrogation) est hachée et divisée par la pondération totale des serveurs en exécution.</p> <p>Le résultat désigne quel serveur reçoit la demande. Ainsi, un URI est toujours dirigé vers le même serveur tant qu'aucun serveur ne se met en marche ou ne s'arrête.</p> <p>Le paramètre d'algorithme de l'URI a deux options : <code>uriLength=<len></code> et <code>uriDepth=<dep></code>. Entrez les paramètres de longueur et de profondeur sur des lignes distinctes dans la zone de texte Paramètres de l'algorithme.</p> <p>Les paramètres de longueur et de profondeur sont suivis d'un nombre entier positif. Ces options peuvent équilibrer des serveurs en fonction du début de l'URI uniquement.</p> <p>Le paramètre de longueur indique que l'algorithme ne doit prendre en compte que les caractères définis au début de l'URI pour calculer le hachage. La plage du paramètre de longueur doit être $1 \leq \text{len} < 256$.</p> <p>Le paramètre de profondeur indique la profondeur de répertoire maximale à utiliser pour calculer le hachage. Un niveau est compté pour chaque barre oblique dans la demande. La plage du paramètre de profondeur doit être $1 \leq \text{dep} < 10$.</p> <p>Si les deux paramètres sont spécifiés, l'évaluation s'arrête lorsque l'un des deux est atteint.</p>

Option	Description et paramètres d'algorithme
HTTPHEADER	<p>Le nom d'en-tête HTTP est recherché dans chaque demande HTTP.</p> <p>Le nom d'en-tête entre parenthèses n'est pas sensible à la casse qui est semblable à la fonction ACL 'hdr()'.</p> <p>Le paramètre d'algorithme HTTPHEADER a une option : <code>headerName=<name></code>. Par exemple, vous pouvez utiliser host comme paramètre d'algorithme HTTPHEADER.</p> <p>Si l'en-tête est absent ou ne contient aucune valeur, l'algorithme Round robin s'applique.</p>
URL	<p>Le paramètre URL spécifié dans l'argument est recherché dans la chaîne de requête de chaque demande HTTP GET.</p> <p>Le paramètre d'algorithme URL a une option : <code>urlParam=<url></code>.</p> <p>Si le paramètre est suivi du signe égal = et d'une valeur, la valeur est hachée et divisée par le poids total des serveurs en cours d'exécution. Le résultat désigne quel serveur reçoit la demande. Ce processus est utilisé pour suivre les identifiants d'utilisateur dans les demandes et s'assurer qu'un même ID d'utilisateur est toujours envoyé au même serveur tant qu'aucun serveur n'est activé ou inactivé.</p> <p>Si aucune valeur ni aucun paramètre n'est trouvé(e), un algorithme Round robin s'applique.</p>

4 (Facultatif) Sélectionnez la méthode de persistance pour ce pool.

La persistance suit et stocke les données de session, par exemple le membre de pool spécifique ayant pris en charge une demande de client. Avec la persistance, les demandes des clients sont dirigées vers le même membre de pool durant toute la durée de vie d'une session ou durant les sessions ultérieures.

Protocole	Méthode de persistance prise en charge
HTTP	Aucun, Cookie, Adresse IP source
HTTPS	Aucun, Adresse IP source et ID de session SSL
TCP	Aucun, Adresse IP source, MSRDp
UDP	Aucun, Adresse IP source

- Sélectionnez **Cookie** pour insérer un cookie unique afin d'identifier la session la première fois qu'un client accède au site. Le cookie est appelé dans les demandes suivantes pour prolonger la connexion au serveur approprié.
- Sélectionnez **Adresse IP source** pour suivre les sessions en fonction de l'adresse IP source. Lorsqu'un client demande une connexion à un serveur virtuel prenant en charge la persistance d'affinité d'adresse source, l'équilibrage de charge vérifie si ce client s'est précédemment connecté, et si c'est le cas, renvoie le client au même membre de pool.
- Sélectionnez **ID de session SSL** et sélectionnez le modèle de trafic HTTPS de relais SSL.
 - Relais SSL - Client -> HTTPS -> LB (relais SSL) -> HTTPS -> serveur

- Client - HTTP-> LB -> HTTP -> serveurs

Remarque vRealize Automation ne prend actuellement en charge que le relais SSL. La méthode de relais SSL est utilisée indépendamment de l'option que vous sélectionnez.

- Sélectionnez **MSRDP** pour maintenir les sessions persistantes entre les clients et les serveurs Windows qui exécutent le service Microsoft Remote Desktop Protocol (RDP). Le scénario recommandé pour activer la persistance MSRDP consiste à créer un pool d'équilibrage de charge composé de membres exécutant Windows Server, dans lequel tous les membres appartiennent à un cluster Windows et à un annuaire de sessions Windows.
 - Sélectionnez **Aucun** pour spécifier que les actions de session ne sont pas stockées pour un rappel suivant.
- 5 Si vous utilisez un paramètre de persistance de cookie, entrez le nom du cookie.
- 6 (Facultatif) Sélectionnez le mode d'insertion du cookie dans le menu déroulant **Mode**.

Option	Description
Insérer	Le dispositif NSX Edge envoie un cookie. Si le serveur envoie un ou plusieurs cookies, le client reçoit un cookie supplémentaire (le ou les cookies du serveur + le cookie NSX Edge). Si le serveur n'envoie aucun cookie, le client reçoit le cookie NSX Edge.
Préfixe	Le serveur envoie un cookie. Utilisez cette option si votre client ne prend pas en charge plusieurs cookies. Si vous employez une application propriétaire utilisant un client propriétaire qui ne prend en charge qu'un seul cookie, le serveur Web envoie un cookie, mais le dispositif NSX Edge injecte (comme préfixe) ses informations de cookie dans la valeur de cookie du serveur.
Session d'application	Le serveur n'envoie aucun cookie. Il envoie plutôt les informations de session utilisateur sous forme d'URL. Par exemple, <code>http://mysite.com/admin/UpdateUserServlet;jsessionid=X000X0XXX0XXXX</code> , où <code>jsessionid</code> correspond aux informations de session utilisateur et est utilisé pour la persistance.

- 7 (Facultatif) Entrez le délai d'expiration de persistance pour le cookie en secondes.

Par exemple, pour un équilibrage de charge L7 avec une adresse IP source TCP, l'entrée de persistance expire si aucune nouvelle connexion TCP n'est établie pendant le délai d'expiration spécifié, même si les connexions existantes sont toujours actives.

- 8 (Facultatif) Cliquez sur l'onglet **Contrôle de santé** et passez à la rubrique [Définir les paramètres de vérification de santé d'un serveur virtuel](#) pour continuer à définir le serveur virtuel dans le composant d'équilibrage de charge NSX.

Définir les paramètres de vérification de santé d'un serveur virtuel

En sélectionnant l'option **Personnaliser** dans l'onglet **Général**, vous pouvez spécifier comment, ou dans quelles circonstances, l'équilibrage de charge NSX effectue des contrôles de santé sur les membres du pool dans le serveur virtuel.

Le protocole de contrôle de santé par défaut et les paramètres de port du contrôle de santé correspondent au protocole et aux paramètres de port dans l'onglet **Général**.

Pour plus d'informations à ce sujet, reportez-vous à la section *Créer un moniteur de service* dans la Documentation du produit NSX disponible sur https://www.vmware.com/support/pubs/nsx_pubs.html. Notez que la documentation sur NSX fait référence au membre du serveur virtuel en tant que membre du pool.

Prérequis

Définir les paramètres généraux du serveur virtuel.

Procédure

- 1 (Facultatif) Sélectionnez un protocole de contrôle de santé dans le menu déroulant **Protocole de contrôle de santé** pour spécifier le mode d'accès au membre de pool lorsque l'équilibrage de charge écoute pour déterminer la santé du membre de pool.

Les options de protocole sont **HTTP**, **HTTPS**, **TCP**, **ICMP**, **UDP** et **Aucun**.

Vous pouvez également accepter le protocole par défaut spécifié dans l'onglet Général.

- 2 (Facultatif) Entrez une valeur dans la zone de texte **Port du contrôle de santé** pour spécifier le port sur lequel l'équilibrage de charge écoute pour surveiller la santé du membre du serveur virtuel ou du membre du pool.

Notez que la documentation sur NSX fait référence à un membre de serveur virtuel comme à un membre du pool.

Les protocoles HTTP, HTTPS et TCP peuvent partager un port avec le protocole UDP. Par exemple, si le service 1 utilise TCP, HTTP ou HTTPS sur le port 80, le service 2 peut utiliser UDP sur le port 80. Si le service 1 utilise UDP sur le port 80, le service 2 ne peut pas utiliser UDP sur ce port.

- 3 Entrez la valeur de l'**intervalle** (en secondes) auquel un serveur reçoit une commande ping.
- 4 Entrez la valeur du **délai d'expiration** maximal (en secondes) au bout duquel le serveur doit envoyer une réponse.
- 5 Entrez une valeur pour le **Nombre max. de nouvelles tentatives** correspondant au nombre de fois où le serveur doit recevoir une commande ping avant d'être déclaré comme étant arrêté.
- 6 Spécifiez les paramètres de contrôle de santé supplémentaires en fonction de votre **protocole de contrôle de santé** spécifié.
 - a Entrez la **méthode** à utiliser pour détecter l'état du serveur. Les options sont GET, OPTIONS et POST.
 - b Entrez l'**URL** à utiliser dans la demande pour détecter l'état du serveur. Il s'agit de l'URL qui est utilisée pour les options de méthode GET et POST ("/" par défaut).

- c Dans la zone de texte **Envoyer**, entrez la chaîne à envoyer au serveur après qu'une connexion a été établie.

Dans la zone de texte **Envoyer**, entrez la chaîne à envoyer au serveur après qu'une connexion a été établie.

- d Dans la zone de texte **Recevoir**, entrez la chaîne attendue que le serveur envoie.

Le serveur est considéré comme actif uniquement lorsque la chaîne reçue correspond à cette définition.

La chaîne peut être un en-tête ou être située dans le corps de la réponse.

- 7 Cliquez sur l'onglet **Avancé** et passez à la rubrique [Définir les paramètres avancés de serveur virtuel](#) pour continuer à définir le serveur virtuel dans le composant d'équilibrage de charge NSX.

Pour spécifier des options de journalisation, reportez-vous à la section [Définir les options de journalisation d'équilibrage de charge](#).

Définir les paramètres avancés de serveur virtuel

Lorsque vous sélectionnez l'option **Personnaliser** de l'onglet **Général**, vous pouvez personnaliser le composant d'équilibrage de charge NSX pour spécifier des paramètres tels que le nombre de connexions simultanées qu'un membre de pool unique peut reconnaître et le nombre maximal de connexions simultanées que le serveur virtuel peut traiter.

Prérequis

[Définir les paramètres généraux du serveur virtuel](#).

Procédure

- 1 Entrez une valeur dans la zone de texte **Limite de connexion** pour spécifier le nombre maximal de connexions simultanées dans NSX que le serveur virtuel peut traiter.

Ce paramètre prend en compte toutes les connexions des membres.

Entrez la valeur 0 pour ne spécifier aucune limite.

- 2 Entrez une valeur dans la zone de texte **Limite du taux de connexion** pour spécifier le nombre maximal de demandes de connexion entrantes dans NSX qui peuvent être acceptées par seconde.

Ce paramètre prend en compte toutes les connexions des membres.

Entrez la valeur 0 pour ne spécifier aucune limite.

- 3 (Facultatif) Cochez la case **Activer l'accélération** pour spécifier que chaque adresse IP virtuelle (VIP) utilise l'équilibrage de charge L4 plus rapide plutôt que l'équilibrage de charge L7.

- 4 (Facultatif) Cochez la case **Transparent** pour permettre aux membres du pool d'équilibrage de charge d'afficher l'adresse IP des machines qui appellent l'équilibrage de charge.

Si cette option n'est pas sélectionnée, les membres du pool d'équilibrage de charge voient l'adresse IP source du trafic comme une adresse IP interne d'équilibrage de charge.

- 5 Entrez une valeur dans la zone de texte **Nbre max. de connexions** pour spécifier le nombre maximal de connexions simultanées qu'un membre de pool unique peut reconnaître.

Si le nombre de demandes entrantes est supérieur à cette valeur, les demandes sont mises en file d'attente et ensuite traitées dans leur ordre de réception à la libération des connexions.

Entrez la valeur 0 pour ne spécifier aucune valeur maximale.

- 6 Entrez une valeur dans la zone de texte **Nbre min. de connexions** pour spécifier le nombre minimal de connexions simultanées qu'un membre de pool doit toujours accepter.

Entrez la valeur 0 pour ne spécifier aucune valeur minimale.

- 7 Cliquez sur **OK** pour terminer la définition du serveur virtuel.

- 8 Pour spécifier des options de journalisation, reportez-vous à la section [Définir les options de journalisation d'équilibrage de charge](#), ou cliquez sur **Enregistrer** ou sur **Terminer**.

Définir les options de journalisation d'équilibrage de charge

Vous pouvez définir les types d'actions de journalisation d'équilibrage de charge qui sont capturées et enregistrées dans les journaux d'équilibrage de charge.

Après ou pendant la définition d'un composant d'équilibrage de charge, vous pouvez spécifier un niveau de journalisation pour collecter des journaux de trafic d'équilibrage de charge. Les niveaux de journalisation que vous définissez pour un composant d'équilibrage de charge sur le Blueprint s'appliquent à tous les équilibrages de charge qui sont définis dans le Blueprint.

Les niveaux de journalisation sont Débogage, Info, Avertissement, Erreur et Critique. Les options Débogage et Info consignent les demandes des utilisateurs, tandis que les options Avertissement, Erreur et Critique ne les consignent pas.

Pour plus d'informations sur la journalisation de l'équilibrage de charge de NSX, consultez le *Guide d'administration de NSX*.

Prérequis

[Définir les paramètres d'un membre d'équilibrage de charge.](#)

Procédure

- 1 Sélectionnez l'onglet **Global** sur le composant d'équilibrage de charge dans le canevas de conception.
- 2 Sélectionnez une ou plusieurs options de journalisation dans le menu déroulant **Niveau de journalisation**.

Sélectionnez un niveau de journalisation pour la collecte des journaux du trafic d'équilibrage de charge. Le paramètre s'applique à tous les composants d'équilibrage de charge NSX du Blueprint.

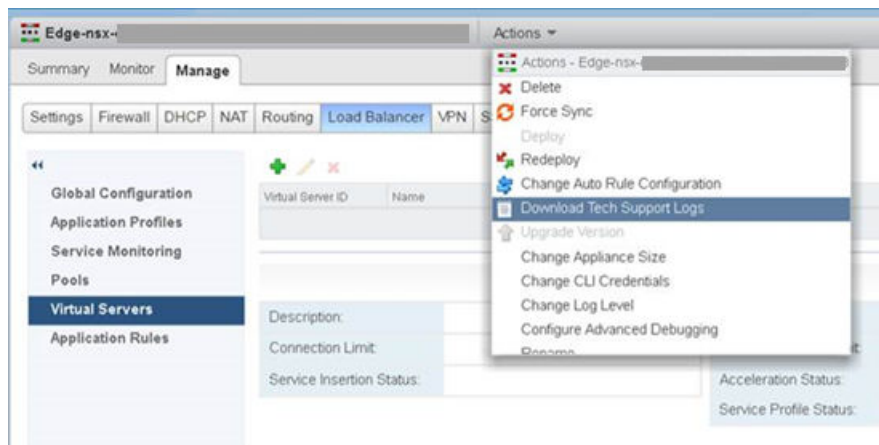
Les paramètres de journalisation sont définis dans le client Web vSphere.

- Aucun
- Info

- Urgence
- Alerte
- Critique
- Erreur
- Avertissement
- Avis
- Débogage

3 Cliquez sur **Enregistrer**.

Vous pouvez afficher et télécharger les journaux dans le client Web vSphere en utilisant le menu **Actions** pour le dispositif NSX Edge comme décrit dans *Télécharger les journaux de support technique pour NSX Edge* dans la documentation du produit NSX disponible sur https://www.vmware.com/support/pubs/nsx_pubs.html.



Utilisation de composants de sécurité dans le canevas de conception

Vous pouvez ajouter des composants de sécurité NSX au canevas pour rendre leurs paramètres configurés disponibles pour un ou plusieurs composants de machine vSphere dans le Blueprint.

Les groupes de sécurité, les balises et les stratégies sont configurés à l'extérieur de vRealize Automation dans l'application NSX.

Les paramètres du composant réseau et de sécurité que vous ajoutez au canevas de conception proviennent de votre configuration NSX et nécessitent l'exécution d'une collecte de données pour l'inventaire NSX pour les clusters vSphere. Les composants réseau et sécurité sont spécifiques à NSX et sont disponibles pour être utilisés avec des composants de machine vSphere uniquement. Pour plus d'informations sur la configuration de NSX, reportez-vous au *Guide d'administration de NSX*.

Vous pouvez ajouter des contrôles de sécurité aux Blueprints en configurant des groupes de sécurité, des balises et des stratégies pour la ressource de calcul vSphere dans NSX. Après avoir exécuté une collecte de données, les configurations de sécurité peuvent être sélectionnées dans vRealize Automation.

Groupe de sécurité

Un groupe de sécurité désigne un ensemble de ressources ou d'objets de groupement issus de l'inventaire vSphere mappé à un ensemble de règles de stratégie de sécurité, par exemple, des règles de pare-feu distribué et des intégrations de services de sécurité de tierce partie, tels que des antivirus et des programmes de détection d'intrusion. La fonctionnalité de regroupement vous permet de créer des conteneurs personnalisés auxquels vous pouvez attribuer des ressources, telles que des machines virtuelles et des adaptateurs réseau, pour la protection par pare-feu distribué. Après avoir défini un groupe, vous pouvez ajouter celui-ci en tant que source ou destination à une règle de pare-feu à des fins de protection.

Vous pouvez ajouter des groupes de sécurité NSX existants ou à la demande à un Blueprint, en plus des groupes de sécurité spécifiés dans la réservation.

Vous pouvez créer un ou plusieurs groupes de sécurité à la demande. Vous pouvez sélectionner une ou plusieurs stratégies de sécurité à configurer sur un groupe de sécurité.

Les groupes de sécurité sont gérés dans la ressource source. Pour plus d'informations sur la gestion des groupes de sécurité de différents types de ressources, reportez-vous à la documentation de NSX.

Si un Blueprint contient un ou plusieurs équilibres de charge et que l'isolation d'application est activée pour le Blueprint, l'équilibrage de charge, les adresses IP virtuelles sont ajoutées au groupe de sécurité de l'isolation d'application comme IPSet. Si un Blueprint contient un groupe de sécurité à la demande qui est associé à un niveau de machine qui est également associé à un équilibrage de charge, le groupe de sécurité à la demande inclut le niveau de la machine et l'IPSet avec l'adresse IP virtuelle de l'équilibrage de charge.

Balise de sécurité

Une balise de sécurité est un objet qualificateur ou une entrée de catégorisation utilisable comme mécanisme de groupement. Vous définissez les critères qu'un objet doit satisfaire pour être ajouté au groupe de sécurité que vous créez. Cela vous confère la possibilité d'inclure des machines en définissant des critères de filtrage avec un certain nombre de paramètres pris en charge pour correspondre aux critères de recherche. Par exemple, vous pouvez ajouter toutes les machines balisées avec une balise de sécurité spécifiée à un groupe de sécurité.

Vous pouvez ajouter une balise de sécurité au canevas de conception.

Stratégie de sécurité

Une stratégie de sécurité est un ensemble de services de point de terminaison, de pare-feu et d'inspection réseau pouvant s'appliquer à un groupe de sécurité. Vous pouvez ajouter des stratégies de sécurité à une machine virtuelle vSphere en utilisant un groupe de sécurité à la demande dans un Blueprint. Vous ne pouvez pas ajouter de stratégie de sécurité directement à une réservation. Après la collecte de données, les règles de sécurité ayant été définies dans NSX pour une ressource de calcul sont disponibles pour être sélectionnés dans un Blueprint.

Isolation d'app

Lorsqu'Isolation d'app est activé, une stratégie de sécurité séparée est créée. L'isolation d'application utilise un pare-feu logique pour bloquer l'ensemble du trafic entrant et sortant vers les applications dans le Blueprint. Les machines de composant provisionnées par un Blueprint contenant une stratégie d'isolation d'application peuvent communiquer entre elles, mais ne peuvent pas se connecter hors du pare-feu, sauf si d'autres groupes de sécurité sont ajoutés au Blueprint avec des stratégies de sécurité autorisant un tel accès.

Ajouter un composant du groupe de sécurité existant

Vous pouvez ajouter un composant du groupe de sécurité NSX existant au canevas de conception en préparation de l'association de ses paramètres avec un ou plusieurs composants de machine ou d'autres types de composants disponibles dans le Blueprint.

Vous pouvez utiliser un composant de groupe de sécurité existant pour ajouter un groupe de sécurité NSX au canevas de conception et configurer ses paramètres à utiliser avec les composants de la machine vSphere et les composants Logiciel ou XaaS qui concernent vSphere.

Vous pouvez ajouter plusieurs composants réseau et de sécurité au canevas de conception.

Prérequis

- Créez et configurez un groupe de sécurité dans NSX. Reportez-vous à la section *Configuration de vRealize Automation* et au Guide d'administration de NSX.
- Vérifiez que l'inventaire NSX a été exécuté avec succès pour votre cluster.
Pour utiliser des configurations NSX dans vRealize Automation, vous devez exécuter la collecte de données.
- Passez en revue les concepts des composants de sécurité. Reportez-vous à [Utilisation de composants de sécurité dans le canevas de conception](#).
- Connectez-vous à la console vRealize Automation en tant qu'**architecte d'infrastructure**.
- Ouvrez un nouveau Blueprint ou un Blueprint existant dans le canevas de conception via l'onglet **Conception**.

Procédure

- 1 Cliquez sur **Réseau et sécurité** dans la section Catégories pour afficher la liste des composants réseau et de sécurité disponibles.
- 2 Faites glisser un composant de **Groupe de sécurité existant** vers le canevas de conception.
- 3 Sélectionnez un groupe de sécurité existant dans le menu déroulant **Groupe de sécurité**.
- 4 Cliquez sur **OK**.
- 5 Cliquez sur **Terminer** pour enregistrer le Blueprint en tant que brouillon ou poursuivez la configuration du Blueprint.

Vous pouvez continuer à configurer des paramètres de sécurité en ajoutant des composants de sécurité supplémentaires et en sélectionnant des paramètres dans l'onglet **Sécurité** d'un composant de machine vSphere dans le canevas de conception.

Ajouter un composant de groupe de sécurité à la demande

Vous pouvez d'ajouter un composant de groupe de sécurité à la demande NSX au canevas de conception en préparation de l'association de ses paramètres avec un ou plusieurs composants de machine vSphere ou d'autres types de composants disponibles dans le Blueprint.

Prérequis

- Créez et configurez une stratégie de sécurité dans NSX. Reportez-vous au guide d'administration de *NSX*.
- Vérifiez que l'inventaire NSX a été exécuté avec succès pour votre cluster.
Pour utiliser des configurations NSX dans vRealize Automation, vous devez exécuter la collecte de données.
- Passez en revue les concepts des composants de sécurité. Reportez-vous à [Utilisation de composants de sécurité dans le canevas de conception](#).
- Connectez-vous à la console vRealize Automation en tant qu'**architecte d'infrastructure**.
- Ouvrez un nouveau Blueprint ou un Blueprint existant dans le canevas de conception via l'onglet **Conception**.

Procédure

- 1 Cliquez sur **Réseau et sécurité** dans la section Catégories pour afficher la liste des composants réseau et de sécurité disponibles.
- 2 Faites glisser un composant de **Groupe de sécurité à la demande** vers le canevas de conception.
- 3 Entrez un nom et, éventuellement, une description.
- 4 Ajouter une ou plusieurs stratégies de sécurité en cliquant sur l'icône Ajouter dans la zone **Stratégies de sécurité** et en sélectionnant les stratégies de sécurité disponibles.
- 5 Cliquez sur **OK**.
- 6 Cliquez sur **Terminer** pour enregistrer le Blueprint en tant que brouillon ou poursuivez la configuration du Blueprint.

Vous pouvez continuer à configurer des paramètres de sécurité en ajoutant des composants de sécurité supplémentaires et en sélectionnant des paramètres dans l'onglet **Sécurité** d'un composant de machine vSphere dans le canevas de conception.

Ajouter un composant de balise de sécurité existant

Vous pouvez ajouter un composant de balise de sécurité NSX au canevas de conception du Blueprint en préparation de l'association de ses paramètres avec un ou plusieurs composants de machine dans le Blueprint.

Vous pouvez utiliser un composant de balise de sécurité pour ajouter une balise de sécurité NSX au canevas de conception et configurer ses paramètres à utiliser avec les composants de machine vSphere et les composants Logiciel qui concernent vSphere.

Vous pouvez ajouter plusieurs composants réseau et de sécurité au canevas de conception.

Prérequis

- Créez et configurez des balises de sécurité dans NSX. Reportez-vous à la section *Configuration de vRealize Automation* et au Guide d'administration de NSX.
- Vérifiez que l'inventaire NSX a été exécuté avec succès pour votre cluster.

Pour utiliser des configurations NSX dans vRealize Automation, vous devez exécuter la collecte de données.
- Connectez-vous à la console vRealize Automation en tant qu'**architecte d'infrastructure**.
- Ouvrez un nouveau Blueprint ou un Blueprint existant dans le canevas de conception via l'onglet **Conception**.

Procédure

- 1 Cliquez sur **Réseau et sécurité** dans la section Catégories pour afficher la liste des composants réseau et de sécurité disponibles.
- 2 Faites glisser un composant de **Balise de sécurité existante** vers le canevas de conception.
- 3 Cliquez dans la zone de texte **Balise de sécurité** et sélectionnez une balise de sécurité existante.
- 4 Cliquez sur **OK**.
- 5 Cliquez sur **Terminer** pour enregistrer le Blueprint en tant que brouillon ou poursuivez la configuration du Blueprint.

Vous pouvez continuer à configurer des paramètres de sécurité en ajoutant des composants de sécurité supplémentaires et en sélectionnant des paramètres dans l'onglet **Sécurité** d'un composant de machine vSphere dans le canevas de conception.

Association de composants de réseau et de sécurité

Vous pouvez faire glisser des composants réseau et de sécurité vers le canevas de conception, de sorte que leurs paramètres soient disponibles lors de la configuration des composants de machine dans le Blueprint. Après que vous avez défini les paramètres réseau et de sécurité de la machine, vous avez la possibilité d'associer des paramètres d'un composant d'équilibrage de charge.

Après avoir ajouté un composant réseau ou de sécurité NSX au canevas de conception et après avoir défini les paramètres disponibles, vous pouvez ouvrir les onglets Réseau et Sécurité d'un composant de machine vSphere dans le canevas et configurer ses paramètres.

Vous pouvez déplacer un composant réseau NAT à la demande vers le canevas de conception et l'associer à un composant de machine vSphere ou à un composant d'équilibrage de charge NSX dans le Blueprint.

Les paramètres du composant réseau et de sécurité que vous ajoutez au canevas de conception proviennent de votre configuration NSX et nécessitent l'exécution d'une collecte de données pour l'inventaire NSX pour les clusters vSphere. Les composants réseau et sécurité sont spécifiques à NSX et sont disponibles pour être utilisés avec des composants de machine vSphere uniquement. Pour plus d'informations sur la configuration de NSX, reportez-vous au *Guide d'administration de NSX*.

Remarque Si un Blueprint contient un ou plusieurs équilibres de charge et que l'isolation d'application est activée pour le Blueprint, l'équilibrage de charge, les adresses IP virtuelles sont ajoutées au groupe de sécurité de l'isolation d'application comme IPSets. Si un Blueprint contient un groupe de sécurité à la demande qui est associé à un niveau de machine qui est également associé à un équilibrage de charge, le groupe de sécurité à la demande inclut le niveau de la machine et l'IPSet avec l'adresse IP virtuelle de l'équilibrage de charge.

Pour plus d'informations sur l'utilisation de règles NAT pour permettre à un port TCP ou UDP de mapper entre l'adresse IP externe d'un dispositif Edge (port source) et une adresse IP privée dans le composant réseau NAT (port cible), reportez-vous à la section [Création et utilisation de règles NAT](#).

Utiliser des composants de conteneur dans les Blueprints

Vous pouvez configurer et utiliser des composants de conteneur dans le Blueprint.

Après qu'un administrateur de conteneur a créé des définitions de conteneur dans Conteneurs pour vRealize Automation, un architecte de conteneur peut ajouter et configurer des composants de conteneur pour les Blueprints vRealize Automation dans le canevas de conception.

Paramètres du composant de conteneur

Vous pouvez configurer les paramètres et les options de Blueprint pour un composant de conteneur Conteneurs pour vRealize Automation dans le canevas de conception vRealize Automation.

Onglet Général

Configurez les paramètres généraux du composant conteneur du Blueprint dans le canevas de conception.

Tableau 3-34. Paramètres de l'onglet Général

Configuration	Description
Nom	Entrez le nom du composant de votre conteneur dans le Blueprint.
Description	Résumez le composant de votre conteneur à l'attention d'autres architectes.
Image	Entrez le nom complet d'une image dans un registre géré, tel qu'un registre privé ou le registre Docker Hub, par exemple <code>registry.hub.docker.com/library/python</code> .

Tableau 3-34. Paramètres de l'onglet Général (suite)

Configuration	Description
Commandes	Entrez une commande qui s'applique à l'image spécifiée, telle que python app.py. Cette commande s'exécute lorsque le processus de provisionnement du conteneur est démarré.
Liens	Les liens offrent une autre façon de connecter des conteneurs sur un hôte unique ou entre plusieurs hôtes. Entrez un ou plusieurs services dans lesquels ce conteneur doit être lié, tels que redis ou datadog.

Onglet Réseau

Configurez les paramètres réseau du composant de conteneur Blueprint dans le canevas de conception.

Vous pouvez attacher un conteneur à un réseau. Le réseau est représenté en tant que composant réseau de conteneur dans le canevas de conception. Les informations sur les réseaux disponibles sont spécifiées sur la page Réseau du formulaire de composant de conteneur.

Tableau 3-35. Paramètres de l'onglet Réseau

Configuration	Description
Réseaux	Spécifiez les réseaux existants qui sont définis pour l'image sélectionnée. Vous pouvez également créer un réseau. Lorsque vous ajoutez un composant de conteneur réseau dans le formulaire de conception, les réseaux que vous spécifiez ici apparaissent en tant qu'options sélectionnables.
Liaisons des ports	Spécifiez les liaisons des ports pour le réseau sélectionné. Ces liaisons peuvent être un hôte de protocole, un port hôte et un port de conteneur.
Publier tous les ports	Cochez cette case pour rendre les ports utilisés dans l'image de conteneur visibles par tous les utilisateurs.
Nom d'hôte	Spécifiez le nom d'hôte du conteneur. Si aucun nom n'est spécifié, cette valeur reprend par défaut le nom du composant de conteneur dans le Blueprint.
Mode réseau	Spécifiez la pile réseau du conteneur. Si aucune valeur n'est spécifiée, le conteneur est configuré en mode réseau bridgé.

Onglet Stockage

Configurez les paramètres de stockage du composant de conteneur Blueprint dans le canevas de conception.

Tableau 3-36. Paramètres de l'onglet Stockage

Paramètres	Description
Volumes	Spécifiez les volumes de stockage qui sont mappés depuis l'hôte pour être utilisés par le conteneur.
Volumes depuis	Spécifiez les volumes de stockage devant être hérités depuis un autre conteneur.
Répertoire de travail	Spécifiez le répertoire depuis lequel exécuter des commandes.

Onglet Stratégie

Configurez des paramètres de stratégie, tels que des stratégies de déploiement et des contraintes d'affinité pour le composant conteneur du Blueprint dans le canevas de conception.

Tableau 3-37. Paramètres de l'onglet Stratégie

Paramètres	Description
Stratégie de déploiement	Spécifiez une stratégie de déploiement pour définir les préférences régissant l'ensemble d'hôtes à utiliser lors du déploiement de ce conteneur. Vous pouvez associer des stratégies de déploiement aux définitions d'hôtes, de stratégies et de conteneur, afin de créer une préférence pour les hôtes, les stratégies et les quotas lors du déploiement d'un conteneur. Les stratégies de déploiement s'ajoutent depuis l'onglet Conteneurs dans vRealize Automation.
Taille du cluster	Spécifiez le nombre d'instances à générer en tant que cluster depuis ce conteneur.
Stratégie de redémarrage	Spécifiez une stratégie de redémarrage pour définir la manière dont un conteneur est redémarré lors d'une sortie.
Max. de redémarrages	Si vous avez sélectionné Lors d'un échec comme stratégie de redémarrage, vous pouvez spécifier le nombre maximal de redémarrages.
Partages de CPU	Spécifiez le nombre de partages de CPU affectés pour la ressource provisionnée.
Limite de mémoire	Spécifiez un nombre minimal compris entre 0 et la mémoire disponible dans la zone de positionnement. Il s'agit de la mémoire totale disponible pour les ressources dans ce positionnement. 0 signifie qu'il n'y a pas de limite.

Tableau 3-37. Paramètres de l'onglet Stratégie (suite)

Paramètres	Description
Échange de mémoire	Limite totale de la mémoire.
Contraintes d'affinité	<p>Définit les règles de provisionnement des conteneurs sur les mêmes hôtes ou des hôtes différents.</p> <ul style="list-style-type: none"> ■ Type d'affinité <p>Pour l'anti-affinité, les conteneurs sont placés dans des hôtes différents. Ils sont placés sur le même hôte dans tous les autres cas.</p> ■ Service <p>Le nom de service qui est disponible dans le menu déroulant correspond au nom de composant de conteneur spécifié dans le champ Nom de l'onglet Général.</p> ■ Contrainte <p>Une contrainte inconditionnelle est une contrainte qui fera échouer le provisionnement si ses conditions ne sont pas réunies. Une contrainte conditionnelle est une contrainte qui permet de poursuivre le provisionnement même si ses conditions ne sont pas réunies.</p>

Onglet Environnement

Configurez les paramètres d'environnement, tels que les liaisons de propriété du composant de conteneur Blueprint dans le canevas de conception.

Tableau 3-38. Paramètres de l'onglet Environnement

Configuration	Description
Nom	Le nom de la variable.
Liaison	<p>Lier la variable à une autre propriété, qui fait partie du modèle. Lorsque vous sélectionnez la liaison, vous devez entrer une valeur dans la syntaxe</p> <p><code>_resource~TemplateComponent~TemplateComponentProperty</code>.</p>
Valeur	La valeur de la variable d'environnement ou, si vous avez sélectionné la liaison, la valeur de la propriété que vous voulez lier.

Onglet Propriétés

Configurez les propriétés individuelles et les groupes de propriétés personnalisées pour le composant de conteneur Blueprint dans le canevas de conception.

Si vous sélectionnez l'onglet **Groupes de propriétés** et cliquez sur **Ajouter**, les options suivantes deviennent disponibles :

- Propriétés de l'hôte du conteneur avec authentification par certificat
- Propriétés de l'hôte du conteneur avec authentification par utilisateur/mot de passe

Les groupes de propriétés qui ont été définis figurent également dans la liste.

Si vous sélectionnez l'onglet **Propriétés personnalisées** et cliquez sur **Ajouter**, vous pouvez ajouter individuellement des propriétés personnalisées au composant de conteneur.

Tableau 3-39. Paramètres de l'onglet Propriétés pour les propriétés personnalisées

Configuration	Description
Nom	Entrez le nom d'une propriété personnalisée ou sélectionnez une propriété personnalisée disponible dans le menu déroulant.
Valeur	Entrez ou modifiez une valeur à associer au nom de la propriété personnalisée.
Chiffré	Vous pouvez choisir de chiffrer la valeur de la propriété, par exemple, si la valeur est un mot de passe.
Remplaçable	Vous pouvez spécifier que la valeur de la propriété peut être remplacée par la prochaine personne qui utilise la propriété. Il s'agit généralement d'un autre architecte, mais si vous sélectionnez Afficher dans la demande, vos utilisateurs peuvent voir et modifier les valeurs des propriétés lorsqu'ils demandent des éléments du catalogue.
Afficher dans la demande	Si vous souhaitez afficher le nom et la valeur de la propriété pour vos utilisateurs finaux, vous pouvez indiquer d'afficher la propriété sur le formulaire de demande lors de la demande de provisionnement de machine. Vous devez également sélectionner Remplaçable si vous souhaitez que les utilisateurs fournissent une valeur.

Onglet Configuration santé

Spécifiez un mode de configuration de santé pour le composant de conteneur de Blueprint dans le canevas de conception.

Tableau 3-40. Paramètres de l'onglet Configuration santé

Paramètres du mode	Description
Aucun	Par défaut. Aucun contrôle de santé n'est configuré.
HTTP	Si vous sélectionnez HTTP , vous devez fournir une API d'accès, ainsi qu'une méthode et une version HTTP à utiliser. L'API est relative et il est superflu d'entrer l'adresse du conteneur. Vous pouvez également spécifier une période de délai d'attente pour l'opération et définir des seuils de santé. Par exemple, un seuil de santé ayant la valeur 2 signifie que deux appels réussis consécutifs doivent se produire pour que le conteneur soit considéré comme sain et passer à l'état EN COURS D'EXÉCUTION. Un seuil de défautuosité ayant la valeur 2 signifie que deux appels non-réussis consécutifs doivent se produire pour que le conteneur soit considéré comme défectueux et passer à l'état ERREUR. Pour tous les états intermédiaires, l'état du conteneur devient DÉTÉRIORÉ.

Tableau 3-40. Paramètres de l'onglet Configuration santé (suite)

Paramètres du mode	Description
Connexion TCP	Si vous sélectionnez Connexion TCP , vous ne devez entrer que le port du conteneur. Le contrôle de santé tente d'établir une connexion TCP avec le conteneur sur le port fourni. Vous pouvez également spécifier une valeur de délai d'attente pour l'opération et définir des seuils de santé et de défectuosité comme pour l'option HTTP.
Commande	Si vous sélectionnez Commande , vous devez entrer une commande à exécuter sur le conteneur. Le succès du contrôle de santé est déterminé par l'état de sortie de la commande.
Ignorer le contrôle de santé lors du provisionnement	Décochez cette option pour forcer le contrôle de santé lors du provisionnement. Si ce contrôle est forcé, un conteneur n'est pas considéré comme étant provisionné tant qu'un contrôle de santé n'a pas réussi.
Autodeploy	Redéploiement automatique des conteneurs présentant l'état ERREUR.

Onglet Configuration journal

Spécifiez un mode de journalisation, ainsi que des options de journalisation facultatives, pour le composant de conteneur de Blueprint dans le canevas de conception.

Tableau 3-41. Paramètres de l'onglet Configuration journal

Configuration	Description
Pilote	Sélectionnez un format de journalisation dans le menu déroulant.
Options	Entrez les options du pilote en utilisant un nom et un format de valeur correspondant au format de journalisation.

Utilisation de propriétés de conteneur et de groupes de propriétés dans un Blueprint

Vous pouvez ajouter des groupes de propriétés prédéfinis à un composant de conteneurs dans un Blueprint vRealize Automation. Lorsque des machines sont provisionnées en utilisant un Blueprint contenant ces propriétés, elles sont enregistrées en tant que machines hôtes de conteneur du Docker.

Conteneurs pour vRealize Automation a fourni les deux groupes de propriétés personnalisées spécifiques aux conteneurs suivantes. Lorsque vous ajoutez un composant de conteneur à un Blueprint, vous pouvez ajouter ces groupes de propriétés au conteneur pour enregistrer les machines provisionnées en tant qu'hôtes de conteneur.

- Propriétés de l'hôte du conteneur avec authentification par certificat
- Propriétés de l'hôte du conteneur avec authentification par utilisateur/mot de passe

Ces groupes de propriétés apparaissent dans vRealize Automation lorsque vous sélectionnez **Administration > Dictionnaire des propriétés > Groupes de propriétés**.

Étant donné que les groupes de propriétés sont partagés par tous les locataires, si vous travaillez dans un environnement à locataires multiples, pensez à cloner et personnaliser vos propriétés. En donnant un nom unique aux groupes de propriétés et aux propriétés dans les groupes, vous pouvez les modifier pour définir des valeurs personnalisées à utiliser dans un locataire spécifique.

Les propriétés utilisées le plus couramment sont `Container.Auth.PublicKey` et `Container.Auth.PrivateKey`, dans lesquelles l'administrateur de conteneurs fournit le certificat client pour s'authentifier sur l'hôte de conteneur.

Tableau 3-42. Propriétés personnalisées Conteneurs

Propriété	Description
<code>containers.ipam.driver</code>	À utiliser uniquement avec des conteneurs. Spécifie le pilote IPAM à utiliser lors de l'ajout d'un composant réseau Conteneurs à un Blueprint. Les valeurs prises en charge dépendent des pilotes installés dans l'environnement hôte des conteneurs dans lequel ils sont utilisés. Par exemple, une valeur prise en charge peut être <code>infoblox</code> ou <code>calico</code> selon les plug-ins IPAM qui sont installés sur l'hôte des conteneurs.
<code>containers.network.driver</code>	À utiliser uniquement avec des conteneurs. Spécifie le pilote réseau à utiliser lors de l'ajout d'un composant réseau Conteneurs à un Blueprint. Les valeurs prises en charge dépendent des pilotes installés dans l'environnement hôte des conteneurs dans lequel ils sont utilisés. Par défaut, les pilotes réseau fournis par le Docker incluent Bridge, Overlay et Macvlan, tandis que les pilotes réseau fournis par VCH (Virtual Container Host) incluent le pilote Bridge. Des pilotes réseau tiers tels que <code>weave</code> et <code>calico</code> peuvent également être disponibles, selon les plug-ins de mise en réseau installés sur l'hôte de conteneur.
<code>Container</code>	À utiliser uniquement avec des conteneurs. La valeur par défaut est <code>App.Docker</code> et elle est obligatoire. Ne modifiez pas cette propriété.
<code>Container.Auth.User</code>	À utiliser uniquement avec des conteneurs. Spécifie le nom d'utilisateur pour se connecter à l'hôte Conteneurs.
<code>Container.Auth.Password</code>	À utiliser uniquement avec des conteneurs. Spécifie le mot de passe du nom d'utilisateur ou celui de la clé publique ou privée à utiliser. La valeur de propriété chiffrée est prise en charge.
<code>Container.Auth.PublicKey</code>	À utiliser uniquement avec des conteneurs. Spécifie la clé publique pour se connecter à l'hôte Conteneurs.
<code>Container.Auth.PrivateKey</code>	À utiliser uniquement avec des conteneurs. Spécifie la clé privée pour se connecter à l'hôte Conteneurs. La valeur de propriété chiffrée est prise en charge.
<code>Container.Connection.Protocol</code>	À utiliser uniquement avec des conteneurs. Spécifie le protocole de communication. La valeur par défaut est <code>API</code> et elle est obligatoire. Ne modifiez pas cette propriété.
<code>Container.Connection.Scheme</code>	À utiliser uniquement avec des conteneurs. Spécifie le schéma de communication. La valeur par défaut est <code>https</code> .

Tableau 3-42. Propriétés personnalisées Conteneurs (suite)

Propriété	Description
Container.Connection.Port	À utiliser uniquement avec des conteneurs. Spécifie le port de connexion Conteneurs. La valeur par défaut est 2376.
Extensibility.Lifecycle.Properties.VMPSMasterWorkf low32.MachineActivated	À utiliser uniquement avec des conteneurs. Spécifie la propriété Broker d'événement pour exposer toutes les propriétés Conteneurs et permet d'enregistrer un hôte provisionné. La valeur par défaut est Container* et elle est obligatoire. Ne modifiez pas cette propriété.
Extensibility.Lifecycle.Properties.VMPSMasterWorkf low32.Disposing	À utiliser uniquement avec des conteneurs. Spécifie la propriété Broker d'événement pour exposer toutes les propriétés Conteneurs ci-dessus et permet de désenregistrer un hôte provisionné. La valeur par défaut est Container* et elle est obligatoire. Ne modifiez pas cette propriété.

Utilisation de composants réseau Conteneurs dans le canevas de conception

Vous pouvez ajouter un ou plusieurs composants réseau Conteneurs au canevas de conception et configurer leurs paramètres pour les composants de machine vSphere dans le Blueprint.

Vous pouvez ajouter les propriétés `containers.ipam.driver` et `containers.network.driver` au composant lorsque vous l'ajoutez au Blueprint.

Ajouter un composant réseau de conteneur

Vous pouvez ajouter des informations réseau de conteneur à un Blueprint vRealize Automation contenant des composants de conteneur.

Vous pouvez configurer les conteneurs dans Conteneurs pour vRealize Automation en utilisant l'onglet vRealize Automation **Conteneurs**. Vous pouvez ajouter ces conteneurs et leurs paramètres réseau en tant que composants dans un Blueprint en utilisant les options de l'onglet vRealize Automation **Concevoir**.

Prérequis

- Connectez-vous à la console vRealize Automation en tant qu'**architecte de conteneur**.
- Ouvrez un nouveau Blueprint ou un Blueprint existant dans le canevas de conception via l'onglet **Conception**.

Procédure

- 1 Cliquez sur **Réseau et sécurité** dans la section Catégories pour afficher la liste des composants réseau et de sécurité disponibles.
- 2 Faites glisser un composant de **Réseau du conteneur** vers le canevas de conception.
- 3 Entrez un nom dans la zone de texte **Nom**, afin de créer un nom unique pour le composant dans le canevas de conception.
- 4 (Facultatif) Entrez une description du composant dans la zone de texte **Description**.

- 5 (Facultatif) Cochez la case **Externe** si vous ne souhaitez pas spécifier de paramètres IPAM externes.

Si vous cochez la case **Externe**, l'onglet **Configuration IPAM** est supprimé.

- 6 Cliquez sur l'onglet **Configuration IPAM** pour spécifier un nouveau sous-réseau ou modifier le sous-réseau existant, la plage IP et la passerelle du réseau spécifié dans un composant de conteneur du Blueprint.

La configuration IPAM s'applique aux nouveaux réseaux créés par vRealize Automation, par opposition à ceux qui ont été créés précédemment dans Docker ou toute autre application de conteneur prise en charge. Ces paramètres ne sont pas validés et le provisionnement échoue si les paramètres chevauchent ceux d'autres réseaux. Par exemple, le sous-réseau et la passerelle doivent être uniques dans l'hôte de conteneur.

- 7 Cliquez sur l'onglet **Propriétés** pour spécifier les propriétés personnalisées du composant.

Si vous sélectionnez l'onglet **Groupes de propriétés** et cliquez sur **Ajouter**, les options suivantes deviennent disponibles :

- Propriétés de l'hôte du conteneur avec authentification par certificat
- Propriétés de l'hôte du conteneur avec authentification par utilisateur/mot de passe

Les groupes de propriétés qui ont été définis figurent également dans la liste.

Si vous sélectionnez l'onglet **Propriétés personnalisées** et cliquez sur **Ajouter**, vous pouvez ajouter individuellement des propriétés personnalisées au composant de conteneur.

Tableau 3-43. Paramètres de l'onglet **Propriétés pour les propriétés personnalisées**

Configuration	Description
Nom	Entrez le nom d'une propriété personnalisée ou sélectionnez une propriété personnalisée disponible dans le menu déroulant.
Valeur	Entrez ou modifiez une valeur à associer au nom de la propriété personnalisée.
Chiffré	Vous pouvez choisir de chiffrer la valeur de la propriété, par exemple, si la valeur est un mot de passe.
Remplaçable	Vous pouvez spécifier que la valeur de la propriété peut être remplacée par la prochaine personne qui utilise la propriété. Il s'agit généralement d'un autre architecte, mais si vous sélectionnez Afficher dans la demande, vos utilisateurs peuvent voir et modifier les valeurs des propriétés lorsqu'ils demandent des éléments du catalogue.
Afficher dans la demande	Si vous souhaitez afficher le nom et la valeur de la propriété pour vos utilisateurs finaux, vous pouvez indiquer d'afficher la propriété sur le formulaire de demande lors de la demande de provisionnement de machine. Vous devez également sélectionner Remplaçable si vous souhaitez que les utilisateurs fournissent une valeur.

- 8 Cliquez sur **Terminer** pour enregistrer le Blueprint en tant que brouillon ou poursuivez la configuration du Blueprint.

Suivant

Vous pouvez poursuivre la configuration des paramètres réseau d'un conteneur depuis l'onglet **Réseau** d'un composant de conteneur dans le canevas de conception.

Transférer des modèles de conteneur pour les utiliser dans des Blueprints

Vous pouvez rendre un modèle de conteneur disponible pour l'utiliser dans un Blueprint vRealize Automation.

Un modèle de conteneur peut inclure plusieurs conteneurs. Lorsque vous transférez un modèle à plusieurs conteneurs dans vRealize Automation, le modèle est créé en tant que Blueprint à plusieurs composants dans vRealize Automation.

Les propriétés spécifiques aux conteneurs que vous ajoutez au modèle sont reconnues dans le Blueprint vRealize Automation. Reportez-vous à [Utilisation de propriétés de conteneur et de groupes de propriétés dans un Blueprint](#).

Lorsque vous demandez le provisionnement d'un Blueprint publié dans le catalogue vRealize Automation, vous provisionnez l'application de conteneurs source de ce Blueprint.

Vous pouvez ajouter d'autres composants au Blueprint vRealize Automation, notamment les types de composants suivants :

- Types de machines
- Composants logiciels
- Autres Blueprints
- Composants réseau et de sécurité NSX
- Composants XaaS
- Composants personnalisés

Vous pouvez transférer un modèle de Conteneurs vers vRealize Automation. Les modifications que vous effectuez dans le Blueprint vRealize Automation ne sont pas répercutées dans le modèle Conteneurs.

Vous pouvez apporter d'autres modifications dans le modèle Conteneurs et le transférer à nouveau pour remplacer le Blueprint dans vRealize Automation. Transférer le modèle dans vRealize Automation remplace le Blueprint, et toutes les modifications apportées au Blueprint dans vRealize Automation entre les transferts sont perdues. Pour éviter de perdre des modifications, utilisez vRealize CloudClient pour cloner un nouveau Blueprint ou pour exporter le Blueprint.

Provisionnement d'un conteneur ou hôte du Docker à partir d'un Blueprint

Vous pouvez créer et utiliser des Blueprints vRealize Automation pour provisionner les machines en tant qu'hôtes de conteneur du Docker enregistré.

Pour qu'une machine puisse être enregistrée en tant qu'hôte de conteneur, elle doit répondre aux exigences suivantes :

- La machine est provisionnée par un Blueprint contenant des propriétés personnalisées spécifiques aux Conteneurs.

Les propriétés personnalisées spécifiques aux conteneurs requises sont fournies dans deux groupes de propriétés. Reportez-vous à [Utilisation de propriétés de conteneur et de groupes de propriétés dans un Blueprint](#).

Pour plus d'informations sur l'utilisation de propriétés personnalisées et de groupes de propriétés dans vRealize Automation, reportez-vous à *Référence des propriétés personnalisées*.

- La machine est accessible sur le réseau.

Par exemple, la machine doit avoir une adresse IP valide et être sous tension.

Vous pouvez définir un Blueprint vRealize Automation pour qu'il contienne des propriétés personnalisées spécifiques qui désignent une machine en tant qu'hôte de conteneur lorsqu'elle est provisionnée à l'aide du Blueprint.

Lorsqu'une machine avec les propriétés du Blueprint requises est provisionnée avec succès, elle est enregistrée dans les Conteneurs et elle reçoit les événements et actions de vRealize Automation.

Création de Blueprints Microsoft Azure et incorporation d'actions sur les ressources

En tant qu'administrateur cloud ou Fabric, vous pouvez créer des Blueprints de machine virtuelle que les administrateurs de groupe d'activité utilisent comme blocs de construction pour créer des machines provisionnées personnalisées pour les consommateurs. Les administrateurs DevOps peuvent également créer des Blueprints de machine Azure ou utiliser ceux qui existent déjà lors de la création de Blueprints composites.

- [Créer un Blueprint pour Microsoft Azure](#)

Vous pouvez créer des Blueprints de machine virtuelle Microsoft Azure permettant d'accéder aux ressources de ces machines.

- [Créer des actions sur les ressources personnalisées Azure](#)

Vous pouvez créer et utiliser des actions sur les ressources personnalisées pour contrôler des machines virtuelles Azure.

Créer un Blueprint pour Microsoft Azure

Vous pouvez créer des Blueprints de machine virtuelle Microsoft Azure permettant d'accéder aux ressources de ces machines.

Un modèle de machine Azure par défaut s'affiche dans la catégorie **Types de machines** sur la page Modifier le Blueprint de vRealize Automation. Vous pouvez utiliser ce modèle de machine virtuelle comme base d'un Blueprint Azure, en suivant la procédure suivante. Après avoir créé un Blueprint Azure, vous pouvez le publier et le déployer tel quel ou l'utiliser avec des ressources Azure personnalisées ou d'autres Blueprints pour créer un Blueprint composite.

Après avoir créé et publié le Blueprint, les utilisateurs disposant des privilèges appropriés peuvent demander et provisionner une instance d'Azure par le biais du catalogue de services de vRealize Automation.

Notez que les Blueprints Azure définissent les exigences de machine virtuelle. vRealize Automation utilise ces exigences pour sélectionner la réservation convenant le mieux au déploiement.

Pour obtenir des informations sur les onglets Paramètres NSX et Propriétés de la boîte de dialogue Nouveau Blueprint, reportez-vous à la section *Configuration de vRealize Automation*.

Si vous souhaitez créer deux machines virtuelles simultanément à partir d'un même déploiement, vous devez créer deux noms d'interfaces réseau et deux noms de machines virtuelles.

Prérequis

- Obtenez un ID d'abonnement Azure valide et les informations connexes, notamment sur le groupe de ressources, le compte de stockage et le réseau virtuel dont vous pouvez avoir besoin pour créer un Blueprint.
- Configurez un point de terminaison Azure pour créer une connexion à Azure qui sera utilisée avec votre déploiement vRealize Automation.
- Configurez les réservations Azure nécessaires à vos groupes d'activités.

Procédure

1 Sélectionnez **Conception > Blueprints**.

2 Cliquez sur l'icône **Nouveau (+)**.

3 Entrez le nom du Blueprint dans la zone de texte **Nom**.

Le nom que vous indiquez est également entré dans la zone de texte **ID**. Dans la plupart des cas, vous pouvez ignorer les onglets **Paramètres NSX** et **Propriétés**.

4 Cliquez sur **OK**.

5 Dans le menu Catégories, cliquez sur **Types de machines**.

6 Faites glisser le modèle de machine virtuelle **Machine Azure** vers le canevas de conception.

Si vous avez créé une ressource Azure personnalisée à utiliser comme base d'un Blueprint, vous pouvez la sélectionner dans la catégorie attribuée dans la liste des catégories.

7 Entrez les informations requises pour la machine virtuelle Azure dans les zones de texte sur les pages à onglets situées dans la partie inférieure du canevas de conception, qui s'affichent en faisant glisser le modèle dans le canevas de conception.

Les choix disponibles pour les zones de texte et autres paramètres de l'ensemble de ces onglets sont déterminés principalement par le point de terminaison Azure configuré en tant que base pour les Blueprints.

Pour la plupart des paramètres, lorsque vous cliquez sur la zone de texte à côté de leur nom, un nouveau volet s'ouvre dans la partie droite de la page. Dans ce volet, vous pouvez entrer les valeurs des paramètres dans la zone de texte **Valeur** et indiquer si elles sont **Requises** ou non. Notez que, dans certains cas, vous pouvez également entrer une **Valeur minimale** et une **Valeur maximale**. Cliquez sur **Appliquer** dans le volet droit pour remplir la zone de texte.

Figure 3-1. Menu de droite du Blueprint Azure

The screenshot shows the 'Azure_Machine_1' configuration window with the 'Storage' tab selected. The 'Resource Group' section has two radio buttons: 'Create New' and 'Use Existing', with 'Use Existing' selected. Below it, the 'Resource Group Name' is 'RG1-vAficionado'. The 'Availability Set' section has three radio buttons: 'None', 'Create New', and 'Use Existing', with 'None' selected. On the right, the 'Required' section has a dropdown set to 'No' and a 'Value' field containing 'RG1-vAficionado'. A red arrow points from the 'Use Existing' radio button to the 'Value' field.

La plupart des paramètres comportent également un bouton **Options avancées**. Ces options vous permettent de définir des longueurs de paramètres et, même, de masquer des paramètres pour des utilisateurs finaux.

Remarque Vous devez remplir les paramètres requis dans chaque onglet afin de procéder à la configuration du Blueprint. Si vous souhaitez laisser un champ vide, vous pouvez revenir en arrière et supprimer l'entrée avant d'enregistrer la configuration.

Onglet	Description	Paramètres importants
Général	Sélectionnez les informations de connexion de base pour la machine virtuelle Azure, par exemple le point de terminaison à utiliser.	<p>ID : identifie la machine virtuelle Azure que vous créez. Si vous modifiez ce nom, l'image de la machine virtuelle Azure dans le canevas de conception est également mise à niveau automatiquement.</p> <p>Description : identifie la machine virtuelle que vous créez et précisez si elle est obligatoire ou pas.</p> <p>Instances : cette sélection permet de créer une machine virtuelle évolutive. Utilisez les champs Minimum et Maximum pour indiquer le nombre d'instances Azure pouvant être générées dynamiquement à partir de cette machine.</p> <p>Utiliser l'authentification du mot de passe : sélectionnez Oui pour utiliser l'authentification du mot de passe, ou Non pour utiliser le SSH.</p> <p>Nom d'utilisateur de l'administrateur : laissez ce champ vide pour qu'il puisse être attribué par l'utilisateur provisionnant la machine.</p> <p>Mot de passe de l'administrateur : laissez ce champ vide ; la personne provisionnant la machine pourra ainsi fournir le mot de passe approprié.</p>
Informations sur le build	Ces champs vous permettent de configurer les informations relatives à la machine virtuelle créée.	<p>Emplacement : sélectionnez l'emplacement géographique où cette machine virtuelle sera déployée.</p> <p>Préfixe de machine : sélectionnez le bouton radio approprié pour indiquer si vous souhaitez utiliser le préfixe de machine du groupe d'activités associé ou créer un préfixe personnalisé. Si vous souhaitez utiliser un préfixe personnalisé, entrez-le dans la zone de texte Préfixe de machine personnalisé.</p> <p>Type d'image de machine virtuelle - Sélectionnez le bouton radio approprié pour l'image de la machine virtuelle : Personnalisée ou Stock. Une machine virtuelle personnalisée est créée à partir du déploiement classique Azure et offre davantage d'options de configuration pour ce qui est des services cloud, des comptes de stockage et des groupes à haute disponibilité.</p> <p>Image de machine virtuelle : identifiez l'image de machine virtuelle Azure sur laquelle le Blueprint sera basé.</p> <ul style="list-style-type: none"> ■ Pour une image de machine virtuelle du stock, l'URN de l'image de la machine doit correspondre au format suivant : (éditeur):(offre):(référence):(version). ■ Pour une image de machine virtuelle personnalisée, l'URN de l'image de la machine doit correspondre au format suivant : <code>https://compte- stockage.blob.core.windows.net/container/image.vhd</code> <p>Pour les images personnalisées, vous devez également renseigner la zone de texte Type d'image de système d'exploitation (Windows ou Linux).</p> <p>Utilisateur Admin : entrez le nom de l'utilisateur admin désigné configuré pour les machines virtuelles basées sur ce Blueprint. Ce champ peut être laissé vide si le nom a été saisi dans le formulaire de demande.</p>

Onglet	Description	Paramètres importants
		<p>Authentification : sélectionnez le bouton radio approprié pour indiquer si les machines virtuelles basées sur ce Blueprint nécessiteront un mot de passe ou l'authentification SSH.</p> <p>Mot de passe de l'administrateur : mot de passe de l'administrateur de l'instance de machine virtuelle.</p> <p>Série : définit la taille totale d'une instance de machine virtuelle. Reportez-vous à la documentation d'Azure à l'adresse https://azure.microsoft.com/fr-fr/documentation/articles/virtual-machines-windows-sizes/ pour obtenir des informations sur la série.</p> <p>Taille : définit la taille de l'instance de machine virtuelle spécifique dans une série. La taille dépend de la série sélectionnée. Si vous disposez d'une connexion valide à une instance d'Azure, les tailles disponibles sont remplies dynamiquement en fonction de l'abonnement et de l'emplacement sélectionné, mais aussi de la série. Reportez-vous à la documentation d'Azure pour obtenir des informations sur la taille.</p> <p>Détails de la taille de l'instance : informations facultatives sur la série et la taille de l'instance de machine virtuelle.</p>

Onglet	Description	Paramètres importants
Ressources de machine	<p>Organisez les ressources de machine virtuelle dans des compartiments. Un groupe de ressources est une construction organisationnelle qui regroupe des ressources de machine virtuelle telles que des sites Web, comptes, bases de données et réseaux.</p> <p>Un groupe à haute disponibilité est un mécanisme permettant de gérer deux machines virtuelles ou plus afin de prendre en charge la redondance. Reportez-vous à la section https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-windows-manage-availability/ pour obtenir plus d'informations sur les groupes à haute disponibilité Azure.</p> <p>Remarque Si vous configurez un Blueprint avec le nombre maximal d'instance Azure défini sur une valeur supérieure à 1, vous devez utiliser le groupe de ressources et le groupe à haute disponibilité existants au lieu d'en créer de nouveaux. L'utilisation de nouveaux groupes de ressources ou groupes à haute disponibilité sur plusieurs instances dans le même déploiement générera des erreurs et d'autres problèmes s'ils sont associés à des équilibrages de charge.</p>	<p>Créer ou réutiliser un groupe de ressources : sélectionnez le bouton radio approprié pour indiquer si vous souhaitez utiliser le groupe de ressources Azure existant ou en créer un nouveau. Le nom du groupe de ressources existant est indiqué sur la page Groupes de ressources dans le portail Azure. Si vous choisissez de créer un nouveau groupe de ressources, un nom approprié pour celui-ci s'affiche automatiquement dans la zone de texte Groupe de ressources.</p> <p>Créer ou réutiliser un groupe à haute disponibilité : sélectionnez le bouton radio approprié en fonction de ce que vous voulez faire. Si vous sélectionnez l'option Créer nouveau, les informations appropriées pour le nouveau groupe à haute disponibilité apparaissent dans la zone de texte.</p>

Onglet	Description	Paramètres importants
Stockage	<p>Ces champs vous permettent d'organiser les comptes de stockage Azure. Un compte de stockage permet d'accéder aux différents types de stockage Azure, tels que blob Azure, tableau de file d'attente et stockage de fichier. Pour la plupart des Blueprints, vous pouvez accepter les valeurs par défaut.</p>	<p>Compte de stockage : entrez le nom du compte de stockage de la machine virtuelle, le cas échéant. Le disque du système d'exploitation de la machine virtuelle Azure est déployé dans ce compte de stockage. Des informations sur les groupes de stockage sont disponibles sur le portail Azure. Vous pouvez avoir plusieurs comptes de stockage.</p> <hr/> <p>Remarque Les noms de comptes de stockage comportant des traits de soulignement ou d'autres caractères spéciaux peuvent être à l'origine d'erreurs.</p> <hr/> <p>Ajouter stockage de diagnostic : cochez cette case si vous utilisez des données de diagnostic avec votre instance Azure.</p> <p>Nombre de disques de stockage : sélectionnez le nombre approprié de disques de stockage des données utilisé avec votre machine virtuelle. Vous pouvez spécifier quatre disques au maximum. Ces disques sont en plus du disque du système d'exploitation spécifié dans la zone de texte Compte de stockage.</p> <p>Nombre de disques de stockage</p> <ul style="list-style-type: none"> ■ Nom du disque : nom attribué au disque. ■ Type de disque : type de périphérique de stockage. ■ Taille du disque : taille de stockage. ■ Réplication : méthode de redondance utilisée pour la sauvegarde du disque. ■ Mise en cache de l'hôte : indique si les opérations de lecture/écriture sont mises en cache pour améliorer les performances.
Réseau	<p>Ces champs vous permettent de sélectionner les options de mise en réseau du Blueprint de machine virtuelle. Pour la plupart des Blueprints, vous pouvez accepter les valeurs par défaut et le consommateur entrera les informations relatives au réseau appropriées lors du déploiement.</p> <hr/> <p>Remarque Vous pouvez créer une seule machine virtuelle par interface, mais chaque machine virtuelle peut avoir jusqu'à quatre interfaces.</p>	<p>Cliquez sur le tableau pour ouvrir la boîte de dialogue située sur la droite et contenant un autre tableau modifiable comportant les champs suivants.</p> <ul style="list-style-type: none"> ■ Nom de l'équilibrage de charge : équilibrage de charge utilisé avec l'instance Azure. ■ Nombre d'interfaces réseau : sélectionnez le nombre d'interfaces réseau utilisées avec l'instance Azure. Le nombre d'interfaces réseau doit être pris en charge par la taille de machine virtuelle sélectionnée dans l'onglet Stockage. ■ Interface réseau : sélectionnez l'interface réseau appropriée au Blueprint de la machine virtuelle. Si vous entrez un réseau existant, vous pouvez ignorer tous les autres onglets Réseau. Si vous entrez un nom d'interface réseau qui n'existe pas, une nouvelle interface réseau avec ce nom est créée et pouvez utiliser les autres onglets Réseau pour la configurer. ■ Préfixe du nom de la carte réseau : préfixe de la carte d'interface réseau. ■ Type d'adresse IP : indique si la machine virtuelle utilise une adresse IP statique ou dynamique.

Onglet	Description	Paramètres importants
		<ul style="list-style-type: none"> ■ Configuration réseau : entrez la configuration réseau appropriée. Les profils réseau sont pris en charge. Il existe deux options : Spécifier des réseaux Azure et Utiliser un profil réseau. Les champs suivants changent en fonction de l'option sélectionnée. ■ Les options suivantes sont disponibles si vous sélectionnez Spécifier des réseaux Azure. Si vous laissez ces zones de texte vides, les constructions de réseau par défaut sont utilisées en fonction des informations spécifiées dans la réservation applicable. <ul style="list-style-type: none"> ■ Nom du réseau virtuel : nom du réseau virtuel. ■ Nom du sous-réseau : nom de domaine du sous-réseau Azure. <hr/> <p>Remarque Vous pouvez définir l'adresse IP publique pour Azure au cours des opérations du jour 2.</p> <hr/> <ul style="list-style-type: none"> ■ Si vous sélectionnez l'option Utiliser un profil réseau, la configuration réseau est détachée des constructions Azure sous-jacentes et est couplée avec le profil de mise en réseau vRealize Automation. <ul style="list-style-type: none"> ■ Si vous laissez la zone de texte Profil réseau vide, le réseau virtuel et le sous-réseau Azure par défaut sont résolus en fonction des réservations applicables pour lesquels un profil réseau est spécifié. ■ Si vous entrez un profil réseau, le réseau virtuel et le sous-réseau Azure sont résolus en fonction de la réservation correspondante.

- 8 Cliquez sur **Terminer** pour enregistrer la configuration du Blueprint et revenir sur la page Blueprints principale.

Suivant

Si vous avez configuré des propriétés personnalisées dans votre réservation Azure pour prendre en charge un tunnel VPN, vous pouvez ajouter des composants logiciels aux Blueprints Azure.

- 1 Sélectionnez les **Composants logiciels** dans le menu Catégories. Les composants logiciels que vous avez configurés pour les Blueprints Azure s'affichent dans le volet inférieur.
- 2 Sélectionnez la machine virtuelle Azure dans les valeurs de la liste déroulante du conteneur.
- 3 Sélectionnez le composant logiciel souhaité et faites-le glisser vers la machine virtuelle Azure sur le canevas de conception.
- 4 S'il existe des propriétés requises pour le composant logiciel, entrez-les dans les zones de texte de paramètres appropriées du canevas de conception ci-dessous.
- 5 Cliquez sur **Enregistrer**.

Si vous souhaitez publier le Blueprint, sélectionnez-le sur la page Blueprints principale et cliquez sur **Publier**. Un Blueprint publié est disponible sur la page Éléments du catalogue. Un gestionnaire de groupe d'activité ou équivalent peut également utiliser ce Blueprint comme base d'un Blueprint composite.

Créer des actions sur les ressources personnalisées Azure

Vous pouvez créer et utiliser des actions sur les ressources personnalisées pour contrôler des machines virtuelles Azure.

La mise en œuvre Azure de vRealize Automation est fournie avec deux actions sur les ressources personnalisées :

- Démarrer une machine virtuelle
- Arrêter une machine virtuelle

En outre, vous pouvez créer des actions sur les ressources personnalisées à l'aide de workflows accessibles par le biais de la bibliothèque de vRealize Orchestrator disponible via l'interface de vRealize Automation.

Vous pouvez utiliser des actions sur les ressources Azure comme toute autre action sur les ressources XaaS dans vRealize Automation. Reportez-vous à *Création de Blueprints et d'actions sur les ressources XaaS* et à *Intégration de vRealize Orchestrator dans vRealize Automation* dans *Configuration de vRealize Automation* pour obtenir plus d'informations sur les actions sur les ressources XaaS.

Prérequis

Configurez un point de terminaison Azure valide pour votre déploiement vRealize Automation.

Procédure

- 1 Sélectionnez **Conception > XaaS > Actions sur les ressources**.
- 2 Cliquez sur **Nouveau**.
- 3 Accédez à **Orchestrator > Bibliothèque > Azure** dans la bibliothèque de workflows de vRealize Orchestrator.
- 4 Sélectionnez le dossier et le workflow souhaités.
- 5 Configurez l'action répondant à vos besoins comme vous le feriez pour toute autre action sur les ressources XaaS.

Création de Blueprints vSphere compatibles avec Puppet

Vous pouvez créer des Blueprints vSphere compatibles avec Puppet qui prennent en charge la gestion des machines virtuelles vSphere basée sur Puppet.

La gestion de configuration basée sur Puppet utilise généralement des rôles et des environnements pour définir et gérer la configuration du logiciel. Attention : le sens des termes rôle et environnement dans Puppet diffère du sens informatique plus général.

Un point de terminaison établit une connexion à un déploiement d'entreprise Puppet existant. Lorsque le point de terminaison est créé, vRealize Automation récupère la liste des environnements et des rôles associés aux déploiements spécifiés. Vous pouvez utiliser ces environnements et ces rôles dans des scénarios à liaison précoce ou à liaison tardive lors de la configuration d'un Blueprint de machine virtuelle compatible avec Puppet.

Remarque Actuellement, les composants Puppet sont uniquement pris en charge sur les Blueprints et machines virtuelles vSphere.

Ajouter un composant Puppet à un Blueprint vSphere

Vous pouvez ajouter un composant de gestion de configuration Puppet à un plan vSphere pour faciliter la gestion forcée des machines virtuelles vSphere à l'aide d'un Puppet Master.

L'ajout d'un composant Puppet à un plan vSphere ajoute un agent Puppet aux machines virtuelles créées à partir de ce plan.

Lorsque vous créez des plans vSphere compatibles avec Puppet, vous avez le choix entre la création d'une configuration de liaison précoce ou de liaison tardive.

Avec la liaison précoce, les utilisateurs définissent les paramètres de rôle et d'environnement Puppet pour toutes les machines virtuelles basées sur un plan spécifique lorsque le composant Puppet est ajouté au plan. Ces paramètres restent statiques pendant toute la durée de vie du plan. Pour la liaison tardive, vous disposez de plusieurs options.

- Laissez les zones de texte **Environnement Puppet** et **Rôle Puppet** vides dans le blueprint, et les utilisateurs fourniront ces paramètres au moment de la demande.
- Spécifiez un **environnement Puppet** et laissez la zone **Rôle Puppet** vide. Les utilisateurs doivent spécifier le rôle au moment de la demande.

Prérequis

Créez un plan vSphere approprié. Consultez [Paramètres du composant de machine vSphere](#) pour plus d'informations.

Procédure

- 1 Sélectionnez **Conception > Blueprints**.
- 2 Sélectionnez **Gestion de la configuration** dans le menu Catégories sur la page de conception de plans.
- 3 Sélectionnez le composant Puppet et faites-le glisser vers le composant vSphere sur le canevas de conception.
- 4 Entrez un **ID** et une **description** pour le composant Puppet dans l'onglet Général en bas de la page. L'ID et la description sont arbitraires.
- 5 Cliquez sur l'onglet Serveur.
- 6 Cliquez sur le menu déroulant et sélectionnez le Puppet Master approprié pour le plan.

- 7 Sélectionnez l'**environnement Puppet** et le **rôle Puppet** appropriés si vous souhaitez utiliser la liaison précoce pour ce composant.

Pour configurer la liaison précoce, sélectionnez un environnement et un rôle Puppet. Si vous souhaitez créer un composant avec la liaison tardive, sélectionnez un **environnement Puppet** ou laissez les zones de texte **Environnement Puppet** et **Rôle Puppet** vides, puis cochez les cases **Définir dans le formulaire de demande**.

Remarque Les cases à cocher **Définir dans le formulaire de demande** sont liées. Si vous en sélectionnez une, l'autre est automatiquement sélectionnée.

- 8 Cliquez sur **Terminer** pour enregistrer la configuration du composant Puppet et revenir à la page principale de conception de plans.

Ajoutez la prise en charge de connexion RDP à vos Blueprints de machine Windows

Pour permettre aux administrateurs de catalogue d'autoriser les utilisateurs à se connecter à l'aide de l'action RDP pour les blueprints Windows, ajoutez des propriétés personnalisées RDP au blueprint et faites référence au fichier RDP préparé par l'administrateur système.

Remarque Si votre administrateur Fabric crée un groupe de propriétés qui contient les propriétés personnalisées requises et que vous l'incluez dans votre Blueprint, il n'est pas nécessaire d'ajouter individuellement les propriétés personnalisées au Blueprint.

Prérequis

- Connectez-vous à la console vRealize Automation en tant qu'**administrateur de locataire** ou **gestionnaire de groupes d'activités**.
- Obtenez le nom du fichier RDP personnalisé créé pour vous par votre administrateur système. Reportez-vous à [Créer un fichier Remote Desktop Protocol \(RDP\) personnalisé pour prendre en charge les connexions RDP des machines provisionnées](#).
- Créez au moins un Blueprint de machine Windows.

Procédure

- 1 Sélectionnez **Conception > Blueprints**.
- 2 Pointez vers le Blueprint à mettre à jour et cliquez sur **Édition**.
- 3 Sélectionnez le composant de machine sur votre canevas pour modifier les détails.
- 4 Cliquez sur l'onglet **Propriétés**.
- 5 Cliquez sur l'onglet **Propriétés personnalisées**.

6 Configurez les paramètres RDP.

- a Cliquez sur **Nouvelle propriété**.
- b Entrez le nom des propriétés RDP personnalisées dans la zone de texte **Nom** et les valeurs correspondantes dans la zone de texte **Valeur**.

Option	Description et valeur
(Requis) <code>RDP.File.Name</code>	Spécifie un fichier RDP à partir duquel obtenir les paramètres, par exemple <code>Mes_Paramètres_RDP.rdp</code> . Le fichier doit se trouver dans le sous-répertoire <code>Website\Rdp</code> du répertoire d'installation de vRealize Automation.
(Requis) <code>VirtualMachine.Rdp.SettingN</code>	Spécifie les paramètres RDP à utiliser lors de l'ouverture d'un lien RDP vers la machine. <i>N</i> est un numéro unique permettant de distinguer les paramètres RDP. Par exemple, pour spécifier le niveau d'authentification RDP de telle sorte qu'aucune exigence d'authentification ne soit spécifiée, définissez la propriété personnalisée <code>VirtualMachine.Rdp.Setting1</code> et définissez la valeur sur le niveau d'authentification <code>:3</code> . Pour plus d'informations sur les paramètres RDP disponibles et leur syntaxe correcte, consultez la documentation RDP Microsoft Windows, par exemple Paramètres RDP pour les Services Bureau à distance dans Windows Server .
<code>VirtualMachine.Admin.NameCompletion</code>	Spécifie le nom de domaine qui doit être inclus dans le nom de domaine complet de la machine généré par les fichiers RDP ou SSH pour l'option de l'interface utilisateur Se connecter via RDP ou Se connecter via SSH . Par exemple, définissez la valeur sur <code>myCompany.com</code> pour générer le nom de domaine complet <code>my-machine-name.myCompany.com</code> dans le fichier RDP ou SSH.

- c Cliquez sur **Enregistrer**.

7 Sélectionnez la ligne Blueprint et cliquez sur **Publier**.

Vos administrateurs de catalogue peuvent autoriser les utilisateurs à exécuter l'action **Se connecter via RDP** pour les machines provisionnées depuis votre Blueprint. Si les utilisateurs ne sont pas autorisés à utiliser cette action, ils ne peuvent pas se connecter via RDP.

Scénario : ajouter le plug-in de nettoyage d'Active Directory à votre Blueprint CentOS

En tant qu'architecte IaaS, vous voudrez configurer vRealize Automation pour nettoyer votre environnement Active Directory lorsque des machines provisionnées sont supprimées de vos hyperviseurs. Pour cela, modifiez votre Blueprint CentOS vSphere pour configurer le plug-in de nettoyage d'Active Directory.

En utilisant le plug-in de nettoyage d'Active Directory, vous pouvez spécifier les actions de compte Active Directory suivantes pour qu'elles se réalisent lorsqu'une machine est supprimée d'un hyperviseur :

- Supprimer le compte AD
- Désactiver le compte AD
- Renommer le compte AD
- Déplacer le compte AD vers une autre unité d'organisation d'AD

Prérequis

Remarque Ces informations ne s'appliquent pas à Amazon Web Services.

- Connectez-vous à la console vRealize Automation en tant qu'**architecte d'infrastructure**.
- Collectez les informations suivantes concernant votre environnement Active Directory :
 - Nom d'utilisateur et mot de passe d'un compte Active Directory avec des droits suffisants pour supprimer, désactiver, renommer ou déplacer des comptes AD. Le nom d'utilisateur doit être au format domaine\nom d'utilisateur.
 - (Facultatif) Nom de l'unité d'organisation vers laquelle déplacer les machines détruites.
 - (Facultatif) Préfixe à associer aux machines détruites.
- Créez un Blueprint de machine. Reportez-vous à *Installation et configuration de vRealize Automation pour le scénario Rainpole*.

Procédure

- 1 Sélectionnez **Conception > Blueprints**.
- 2 Pointez vers un Blueprint **Centos sur vSphere** et cliquez sur **Modifier**.
- 3 Sélectionnez le composant de machine sur votre canevas pour dévoiler l'onglet de détails.
- 4 Cliquez sur l'onglet **Propriétés**.
- 5 Cliquez sur **propriétés personnalisées** pour configurer le plug-in de nettoyage d'Active Directory.
 - a Cliquez sur **Nouvelle propriété**.
 - b Tapez `Plugin.AdMachineCleanup`. Exécutez dans la zone de texte **Nom**.
 - c Tapez `vrai` dans la zone de texte **Valeur**.
 - d Cliquez sur l'icône **Enregistrer** (✓).
- 6 Configurez le plug-in de nettoyage d'Active Directory en ajoutant des propriétés personnalisées.

Option	Description et valeur
<code>Plugin.AdMachineCleanup.UserName</code>	Saisissez le nom d'utilisateur du compte Active Directory dans la zone de texte Valeur . Cet utilisateur doit posséder les autorisations suffisantes pour supprimer, désactiver, déplacer et renommer des comptes Active Directory. Le nom d'utilisateur doit être au format domaine\nom d'utilisateur.
<code>Plugin.AdMachineCleanup.Password</code>	Saisissez le mot de passe correspondant au nom d'utilisateur du compte Active Directory dans la zone de texte Valeur .
<code>Plugin.AdMachineCleanup.Delete</code>	Définissez cette valeur sur True pour supprimer les comptes des machines détruites au lieu de les désactiver.

Option	Description et valeur
<code>Plugin.AdMachineCleanup.MoveToOu</code>	Déplacez le compte des machines détruites vers une nouvelle unité d'organisation Active Directory. La valeur est l'unité d'organisation vers laquelle vous déplacez le compte. Cette valeur doit être dans le format <code>ou=UO, dc=dc</code> , par exemple <code>ou=trash,cn=computers,dc=lab,dc=local</code> .
<code>Plugin.AdMachineCleanup.RenamePrefix</code>	Renomme les comptes des machines détruites en ajoutant un suffixe. La valeur est la chaîne du préfixe qui doit être ajouté, par exemple <code>détruite_</code> .

7 Cliquez sur **OK**.

Lorsque des machines provisionnées depuis votre Blueprint sont supprimées de votre hyperviseur, votre environnement Active Directory est mis à jour.

Scénario : permettre aux demandeurs de spécifier un nom d'hôte de machine

En tant qu'architecte de Blueprint, vous voudrez autoriser vos utilisateurs à choisir leurs propres noms de machines lorsqu'ils demandent vos Blueprints. Pour cela, modifiez votre Blueprint vSphere CentOS pour ajouter la propriété personnalisée de nom d'hôte et configurez-la afin d'inviter les utilisateurs à saisir une valeur lors de leurs demandes.

Remarque Si votre administrateur Fabric crée un groupe de propriétés qui contient les propriétés personnalisées requises et que vous l'incluez dans votre Blueprint, il n'est pas nécessaire d'ajouter individuellement les propriétés personnalisées au Blueprint.

Prérequis

- Connectez-vous à la console vRealize Automation en tant qu'**architecte d'infrastructure**.
- Créez un Blueprint de machine. Reportez-vous à *Installation et configuration de vRealize Automation pour le scénario Rainpole*.

Procédure

- 1 Sélectionnez **Conception > Blueprints**.
- 2 Pointez vers un Blueprint **Centos sur vSphere** et cliquez sur **Modifier**.
- 3 Sélectionnez le composant de machine sur votre canevas pour dévoiler l'onglet de détails.
- 4 Cliquez sur l'onglet **Propriétés**.
- 5 Cliquez sur **Nouvelle propriété**.
- 6 Entrez le **nom d'hôte** dans la zone de texte **Nom**.
- 7 Laissez la zone de texte **Valeur**.

- 8 Configurer vRealize Automation pour inviter les utilisateurs à entrer une valeur de nom d'hôte lors de leur demande.

- a Sélectionnez l'option **Remplaçable**.
- b Sélectionnez **Afficher dans la demande**.

Comme les noms d'hôtes doivent être uniques, les utilisateurs ne peuvent demander qu'une seule machine à la fois depuis ce Blueprint.

- 9 Cliquez sur l'icône **Enregistrer** (✓).

- 10 Cliquez sur **OK**.

Les utilisateurs qui demandent une machine depuis votre Blueprint doivent spécifier un nom d'hôte pour leur machine. vRealize Automation valide le fait que le nom d'hôte spécifié est unique.

Scenario : permettre aux utilisateurs de sélectionner des emplacements de centre de données pour des déploiements inter-région

En tant qu'architecte de Blueprint, vous souhaitez autoriser les utilisateurs à choisir si le provisionnement des machines doit s'effectuer sur l'infrastructure de Boston ou de Londres. À cette fin, modifiez le Blueprint CentOS vSphere existant pour activer la fonctionnalité des emplacements.



Vous voulez éviter que les utilisateurs du centre de données de Boston ne provisionnent des machines de l'infrastructure de Londres, et que les utilisateurs du centre de données de Londres ne provisionnent des machines de l'infrastructure de Boston. Pour vous assurer que les utilisateurs de Boston ne provisionnent que l'infrastructure de Boston, et ceux de Londres celle de Londres uniquement, vous souhaitez autoriser les utilisateurs à sélectionner l'emplacement de provisionnement adéquat lors de leur demande de machines.

Prérequis

- Connectez-vous à la console vRealize Automation en tant qu'**architecte d'infrastructure**.
- En tant qu'administrateur système, définissez les emplacements de centre de données. Reportez-vous à [Scénario : ajouter des emplacements de centre de données pour des déploiements inter-région](#).
- En tant qu'administrateur Fabric, appliquez les emplacements appropriés aux ressources de calcul. Reportez-vous à [Scénario : appliquer un emplacement à une ressource de calcul pour des déploiements inter-région](#).

- Créez un Blueprint de machine. Reportez-vous à *Installation et configuration de vRealize Automation pour le scénario Rainpole*.

Procédure

- 1 Sélectionnez **Conception > Blueprints**.
- 2 Pointez vers un Blueprint **Centos sur vSphere** et cliquez sur **Modifier**.
- 3 Dans le canevas, sélectionnez le composant de machine pour afficher l'onglet **Détails généraux**.
- 4 Cochez la case **Afficher l'emplacement à la demande**.
- 5 Cliquez sur **Terminer**.
- 6 Pointez vers le Blueprint **Centos sur vSphere** et cliquez sur **Publier**.

Les utilisateurs du groupe d'activité sont à présent invités à sélectionner un emplacement de centre de données lorsqu'ils demandent le provisionnement d'une machine à partir du Blueprint.

Conception de composants Logiciel

En tant qu'architecte de logiciel, vous créez des composants logiciels réutilisables en normalisant les propriétés de configuration et en utilisant des scripts d'action pour spécifier comment les composants sont installés, configurés, désinstallés ou mis à jour lors des opérations de dimensionnement de déploiement. Vous pouvez réécrire ces scripts d'action à tout moment et les publier en direct pour appliquer les modifications aux composants logiciels provisionnés.

Vous pouvez concevoir des scripts d'action génériques et réutilisables en définissant et en utilisant des paires de nom et valeur appelées propriétés logicielles et en les enregistrant dans vos scripts d'action en tant que paramètres. Si vos propriétés logicielles contiennent des valeurs qui sont inconnues ou qui doivent être définies ultérieurement, vous pouvez autoriser des architectes de Blueprints ou des utilisateurs finaux à fournir les valeurs manquantes ou les obliger à le faire. Si vous devez utiliser une valeur d'un autre composant dans un Blueprint, par exemple l'adresse IP d'une machine, vous pouvez lier la propriété logicielle à la propriété de l'adresse IP de cette machine. L'utilisation de propriétés logicielles pour paramétrer les scripts d'action les rend génériques et réutilisables, de sorte que vous pouvez déployer des composants logiciels dans plusieurs environnements sans modifier vos scripts.

Tableau 3-44. Actions du cycle de vie

Actions du cycle de vie	Description
Installer	Installez votre logiciel. Vous pouvez, par exemple, télécharger une installation du serveur Tomcat et installer un service Tomcat. Les scripts que vous écrivez pour l'action du cycle de vie Installer s'exécutent lorsque le logiciel est provisionné pour la première fois, soit lors d'une demande de déploiement initial, soit dans le cadre d'une montée en charge.
Configurer	Configurez votre logiciel. Dans l'exemple de Tomcat, vous pouvez définir les options JAVA_OPTS et CATALINA_OPTS. Les scripts de configuration s'exécutent une fois l'action Installer terminée.
Démarrer	Démarrez votre logiciel. Vous pouvez, par exemple, démarrer le service Tomcat à l'aide de la commande Démarrer du serveur Tomcat. Les scripts de démarrage s'exécutent une fois l'action Configurer terminée.

Tableau 3-44. Actions du cycle de vie (suite)

Actions du cycle de vie	Description
Mettre à jour	Si vous concevez votre composant logiciel de sorte à ce qu'il prenne en charge des Blueprints évolutifs, gérez les mises à jour requises après une opération de réduction de charge ou de montée en charge. Vous pouvez, par exemple, modifier la taille du cluster pour un déploiement dimensionné et gérer les nœuds en cluster à l'aide d'un équilibrage de charge. Concevez vos scripts de mise à jour de sorte à ce qu'ils s'exécutent plusieurs fois (idempotent) et qu'ils traitent à la fois les cas de réduction de charge et de montée en charge. Lorsqu'une opération de dimensionnement est effectuée, les scripts de mise à jour s'exécutent sur tous les composants logiciels dépendants.
Désinstaller	Désinstallez votre logiciel. Vous pouvez, par exemple, effectuer des actions spécifiques dans l'application avant la destruction d'un déploiement. Les scripts de désinstallation s'exécutent chaque fois que des composants logiciels sont détruits.

Vous pouvez télécharger des composants Logiciel prédéfinis pour différents services intergiciels et applications à partir de VMware Solution Exchange. L'utilisation de l'API REST vRealize CloudClient ou vRealize Automation vous permet d'importer par programmation des composants Logiciel prédéfinis dans votre instance de vRealize Automation.

- Pour consulter la page VMware Solution Exchange, accédez à https://solutionexchange.vmware.com/store/category_groups/cloud-management.
- Pour plus d'informations sur l'API REST vRealize Automation, reportez-vous à *Guide de programmation* et *Référence de l'API de vRealize Automation*.
- Pour plus d'informations sur vRealize CloudClient, reportez-vous à <https://developercenter.vmware.com/tool/cloudclient>.

Types de propriétés et options de paramètres

Vous pouvez concevoir des scripts d'action génériques et réutilisables en définissant et en utilisant des paires de nom et valeur appelées propriétés logicielles et en les enregistrant dans vos scripts d'action en tant que paramètres. Vous pouvez créer des propriétés logicielles qui requièrent des valeurs de type chaîne, groupe, contenu, booléen ou entier. Vous pouvez fournir la valeur vous-même, demander à une autre personne de la fournir ou l'extraire d'un autre composant de Blueprint en créant une liaison.

Options de propriétés

Vous pouvez calculer la valeur de toute propriété de type chaîne en sélectionnant la case à cocher Calculées et vous pouvez rendre toute propriété chiffrée, remplaçable ou obligatoire en sélectionnant les cases à cocher correspondantes lorsque vous configurez les propriétés Logiciel. Combinez ces options à vos valeurs pour atteindre différents objectifs. Exemple : vous voulez que les architectes Blueprint fournissent une valeur de mot de passe et qu'ils la chiffrent lorsqu'ils utilisent votre composant logiciel dans un Blueprint. Créez la propriété de mot de passe, mais laissez la zone de texte vide. Sélectionnez Remplaçable, Requis et Chiffré. Si le mot de passe attendu appartient à votre utilisateur final, l'architecte Blueprint peut sélectionner **Afficher dans la demande** pour obliger les utilisateurs à entrer le mot de passe lorsqu'ils remplissent le formulaire de demande.

Option	Description
Chiffré	Marquez les propriétés comme chiffrées afin de masquer la valeur et de la remplacer par des astérisques dans vRealize Automation. Si vous passez une propriété de chiffrée à non chiffrée, vRealize Automation réinitialise la valeur de la propriété. À des fins de sécurité, vous devez définir une nouvelle valeur pour la propriété.
Remplaçable	Autorisez les architectes à modifier la valeur de cette propriété lorsqu'ils assemblent un Blueprint d'application. Si vous entrez une valeur, elle s'affiche en tant que valeur par défaut.
Obligatoire	Obligez les architectes à fournir une valeur pour cette propriété ou à accepter la valeur par défaut que vous fournissez.
Calculée	Les valeurs des propriétés calculées sont attribuées par les scripts de cycle de vie INSTALLATION, CONFIGURATION, DÉMARRAGE ou MISE À JOUR. La valeur attribuée est propagée aux étapes disponibles suivantes du cycle de vie et aux composants qui sont liés à ces propriétés dans un Blueprint. Si vous sélectionnez la valeur Calculée pour une propriété qui n'est pas une propriété de type chaîne, le type de propriété est changé en chaîne.

Si vous sélectionnez l'option de propriétés calculées, laissez la zone de votre propriété personnalisée vide. Configurez vos scripts pour les valeurs calculées.

Tableau 3-45. Exemples de script pour l'option de propriétés calculées

Exemple de propriété de type chaîne	Syntaxe du script	Exemple d'utilisation
my_unique_id = ""	Bash - \$my_unique_id	<pre>export my_unique_id="0123456789"</pre>
	Windows CMD - %my_unique_id%	<pre>set my_unique_id=0123456789</pre>
	Windows PowerShell - \$my_unique_id	<pre>\$my_unique_id = "0123456789"</pre>

Propriété de type chaîne

Les propriétés de type chaîne requièrent des valeurs de chaîne. Vous pouvez fournir la chaîne vous-même, demander à une autre personne de la fournir ou l'extraire d'un autre composant de Blueprint en créant une liaison avec une autre propriété de type chaîne. Les valeurs de chaîne peuvent contenir n'importe quel caractère ASCII. Pour créer une liaison de propriétés, utilisez l'onglet **Propriétés** du canevas de conception pour sélectionner la propriété appropriée à la liaison. La valeur de la propriété est

ensuite transmise aux scripts d'action en tant que données de chaîne brutes. Lorsque vous effectuez une liaison avec une propriété de type chaîne de Blueprint, assurez-vous que le composant de Blueprint que vous liez ne peut pas être mis en cluster. S'il est mis en cluster, la valeur de chaîne devient une valeur de groupe et vous n'extrayez pas la valeur attendue.

Exemple de propriété de type chaîne	Syntaxe du script	Exemple d'utilisation
admin_email = "admin@email987.com"	Bash - \$admin_email	echo \$admin_email
	Windows CMD - %admin_email%	echo %admin_email%
	Windows PowerShell - \$admin_email	write-output \$admin_email

Propriété de type groupe

Les propriétés de type groupe requièrent un groupe de valeurs de type chaîne, entier, décimale ou booléen sous la forme [*valeur1*, *valeur2*, *valeur3*...]. Vous pouvez fournir les valeurs vous-même, demander à une autre personne de les fournir ou les extraire d'un autre composant de Blueprint en créant une liaison de propriétés.

Lorsque vous créez une propriété logicielle de type tableau, où le type de données est entier ou décimale, vous devez utiliser un point-virgule comme séparateur d'élément de tableau, quels que soient les paramètres régionaux. N'utilisez pas de virgule (,) ou de point (.). Pour certains paramètres régionaux, vous pouvez utiliser une virgule (,) comme séparateur décimal. Par exemple :

- Un tableau valide pour le français ressemble à : [1,11 ; 2,22 ; 3,33]
- Un tableau valide pour l'anglais ressemble à : [1.11,2.22,3.33]

Lorsque vous transmettez de grands nombres dans un tableau, n'utilisez pas le format de regroupement. Par exemple : n'utilisez pas **4444 444.000** (français), **4.444.444,000** (italien) ou **4,444,444.000** (anglais), car les fichiers de données qui contiennent les formats spécifiques peuvent être mal interprétés lors de leur transfert vers une machine qui a d'autres paramètres régionaux. Le format de regroupement n'est pas autorisé, car un nombre tel que **4,444,444.000** est considéré comme trois nombres distincts. Entrez plutôt **4444444.000**.

Lorsque vous définissez les valeurs d'une propriété de type groupe, vous devez mettre le groupe entre crochets. Pour un groupe de chaînes, la valeur des éléments du groupe peut contenir n'importe quel caractère ASCII. Pour coder correctement un caractère de barre oblique inverse dans une valeur de propriété de type Groupe, ajoutez une autre barre oblique inverse, par exemple, ["c:\\test1\\test2"]. Pour une propriété liée, utilisez l'onglet **Propriétés** du canevas de conception pour sélectionner la propriété appropriée à la liaison. Si vous effectuez une liaison avec un groupe, vous devez concevoir vos composants logiciels de sorte que le groupe de valeurs puisse être généré dans n'importe quel ordre.

Par exemple, prenons une machine virtuelle d'équilibrage de charge qui équilibre la charge d'un cluster de machines virtuelles de serveur d'application. Dans ce cas, une propriété de type groupe est définie pour le service d'équilibrage de charge, et elle est définie sur le groupe d'adresses IP des machines virtuelles du serveur d'application.

Ces scripts de configuration du service d'équilibrage de charge utilisent la propriété de type groupe pour configurer le schéma d'équilibrage de charge approprié sur les systèmes d'exploitation Red Hat, Windows et Ubuntu.

Exemple de propriété de type groupe	Syntaxe du script	Exemple d'utilisation
operating_systems = ["Red Hat", "Windows", "Ubuntu"]	Bash - \${operating_systems[@]} pour l'intégralité du groupe de chaînes \${operating_systems[N]} pour l'élément de groupe distinct	for ((i = 0 ; i < \$ {#operating_systems[@]}; i++)); do echo \${operating_systems[i]} done
	Windows CMD - %operating_systems_% où N représente la position de l'élément dans le groupe	for /F "delims== tokens=2" %%A in ('set operating_systems_') do (echo %%A)
	Windows PowerShell - \$operating_systems pour l'intégralité du groupe de chaînes \$operating_systems[N] pour l'élément de groupe distinct	foreach (\$os in \$operating_systems){ write-output \$os }

Propriété de type contenu

La valeur de propriété de type contenu est une URL vers un fichier pour télécharger du contenu. L'agent Logiciel télécharge le contenu à partir de l'URL sur la machine virtuelle et transmet au script l'emplacement du fichier local dans la machine virtuelle.

Les propriétés de type contenu doivent être définies en tant qu'URL valide avec le protocole HTTP ou HTTPS. Par exemple, le composant Logiciel du serveur d'application JBOSS dans l'exemple d'application Dukes Bank spécifie une propriété de contenu cheetah_tgz_url. Les artefacts d'Hyperic sont hébergés dans le dispositif Logiciel et l'URL pointe vers cet emplacement dans le dispositif. L'agent Logiciel télécharge les artefacts à partir de l'emplacement spécifié dans la machine virtuelle déployée.

Pour plus d'informations sur les paramètres software.http.proxy que vous pouvez utiliser avec les propriétés de type contenu, reportez-vous à *Référence des propriétés personnalisées*.

Exemple de propriété de type chaîne	Syntaxe du script	Exemple d'utilisation
cheetah_tgz_url = "http://app_content_server_ip:port/artifacts/software/jboss/cheetah-2.4.4.tar.gz"	Bash - \$cheetah_tgz_url	tar -zxvf \$cheetah_tgz_url
	Windows CMD - %cheetah_tgz_url %	start /wait c:\unzip.exe %cheetah_tgz_url %

Exemple de propriété de type chaîne	Syntaxe du script	Exemple d'utilisation
	Windows PowerShell - \$cheetah_tgz_url	& c:\unzip.exe \$cheetah_tgz_url

Propriété booléenne

Utilisez la propriété de type booléen pour offrir les choix Vrai et Faux dans le menu déroulant Valeur.

Propriété de type entier

Utilisez la propriété de type entier pour les zéros et les entiers positifs ou négatifs.

Propriété de type décimale

Utilisez la propriété de type décimale pour les valeurs représentant des fractions décimales non répétitives.

Cas où votre composant Logiciel doit utiliser les informations d'un autre composant

Dans plusieurs scénarios de déploiement, un composant a besoin de la valeur de propriété d'un autre composant pour se personnaliser. Pour ce faire, vous pouvez utiliser vRealize Automation et créer des liaisons de propriétés. Vous pouvez concevoir vos scripts d'action Logiciel pour les liaisons de propriétés., mais les liaisons réelles sont configurées par l'architecte qui assemble le Blueprint.

Outre le fait de définir une propriété pour une valeur codée de manière irréversible, l'architecte de logiciel, l'architecte IaaS ou l'architecte d'application peut lier des propriétés de composant Logiciel à d'autres propriétés du Blueprint, telles qu'une adresse IP ou un emplacement d'installation. Lorsque vous liez une propriété Logiciel à une autre propriété, vous pouvez personnaliser un script en fonction de la valeur de propriété d'un autre composant ou d'une propriété de machine virtuelle. Par exemple, un composant WAR peut avoir besoin de l'emplacement d'installation du serveur Apache Tomcat. Dans les scripts, vous pouvez configurer le composant WAR afin qu'il définisse la valeur de propriété `server_home` sur celle du serveur Apache Tomcat `install_path` dans le script. La valeur de propriété `server_home` est définie correctement à condition que l'architecte qui assemble le Blueprint lie la propriété `server_home` à la propriété `install_path` du serveur Apache Tomcat.

Vos scripts d'action peuvent uniquement utiliser les propriétés correspondantes que vous définissez et vous pouvez uniquement créer des liaisons de propriétés avec des valeurs de type chaîne et groupe. Comme les groupes de propriétés du Blueprint ne sont pas renvoyés dans un ordre spécifique, la liaison avec des composants évolutifs ou pouvant être mis en cluster risque de ne pas générer les valeurs attendues. Par exemple, votre composant logiciel requiert tous les ID machines d'un cluster de machines et vous autorisez vos utilisateurs à demander un cluster de 1 à 10 et à dimensionner le déploiement de 1 à 10 machines. Si vous configurez votre propriété logicielle comme une propriété de type chaîne, vous obtenez un seul ID machine du cluster, sélectionné de manière aléatoire. Si vous configurez votre propriété logicielle comme une propriété de type de tableau, vous obtenez un groupe de tous les ID machine du cluster, non triés dans un ordre spécifique. Si vos utilisateurs dimensionnent le déploiement,

l'ordre des valeurs peut différer pour chaque opération. Pour vous assurer de ne jamais perdre de valeurs pour les composants mis en cluster, vous pouvez utiliser le type de tableau pour n'importe quelle propriété logicielle. Cependant, vous devez concevoir vos composants logiciels de sorte que le groupe de valeurs puisse être généré dans n'importe quel ordre.

Consultez le tableau Exemples de liaisons de propriétés de type chaîne pour obtenir un aperçu des valeurs de propriétés de type chaîne lors d'une liaison à des types de propriétés différents.

Tableau 3-46. Exemples de liaisons de propriétés de type chaîne

Exemple de type de propriété	Type de propriété pour la liaison	Résultat de la liaison (A est lié à B)
Chaîne (propriété A)	Chaîne (propriété B="Hi")	A="Hi"
Chaîne (propriété A)	Contenu (propriété B="http://my.com/content")	A="http://my.com/content"
Chaîne (propriété A)	Groupe (propriété B=["1", "2"])	A=["1", "2"]
Chaîne (propriété A)	Calculée (propriété B="Hello")	A="Hello"

Consultez le tableau Exemples de liaisons de propriétés de type groupe pour obtenir un aperçu des valeurs de propriétés de type groupe lors d'une liaison à des types de propriétés différents.

Tableau 3-47. Exemples de liaisons de propriétés de type groupe

Exemple de type de propriété	Type de propriété pour la liaison	Résultat de la liaison (A est lié à B)
Groupe (propriété A)	Chaîne (propriété B="Hi")	A="Hi"
Groupe (propriété A)	Contenu (propriété B="http://my.com/content")	A="http://my.com/content"
Groupe (propriété A)	Calculée (propriété B="Hello")	A="Hello"

Pour obtenir une explication détaillée des types de propriétés pris en charge, reportez-vous à [Types de propriétés et options de paramètres](#).

Transfert de valeurs de propriétés entre des étapes de cycle de vie

Vous pouvez modifier et transférer des valeurs de propriétés entre des étapes de cycle de vie au moyen de scripts d'action.

Pour une propriété de type calculée, vous pouvez modifier la valeur d'une propriété et transférer la valeur à la prochaine étape de cycle de vie du script d'action. Par exemple, si le composant A a la valeur `progress_status` définie sur `intermédiaire`, dans l'étape de cycle de vie `INSTALLATION` et `CONFIGURATION` vous pouvez modifier la valeur à `progress_status=installed` dans les scripts d'action respectifs. Si le composant B est associé au composant A, les valeurs de propriétés de `progress_status` des étapes de cycle de vie du script d'action sont identiques à celles du composant A.

Indiquez dans le composant logiciel que le composant B dépend du composant A. Cette dépendance définit le transfert de valeurs de propriétés correctes entre les composants, qu'ils soient dans le même nœud ou dans différents nœuds.

Par exemple, vous pouvez mettre à jour une valeur de propriété dans le script d'action en utilisant les scripts pris en charge.

- Bash `progress_status="completed"`
- Windows CMD `set progress_status=completed`
- Windows PowerShell `$progress_status="completed"`

Remarque Les propriétés de type groupe et contenu ne prennent pas en charge le transfert des valeurs de propriété modifiées entre les scripts d'action des étapes de cycle de vie.

Recommandations concernant le développement de composants

Pour vous familiariser avec les recommandations en matière de définition de propriétés et de scripts d'action, vous pouvez télécharger et importer des composants Logiciel et des Blueprints d'application de VMware Solution Exchange.

Respectez ces recommandations lorsque vous développez des composants Logiciel.

- Pour qu'un script puisse s'exécuter sans interruption, la valeur de retour doit être définie sur zéro (0). Ce paramètre permet à l'agent de capturer toutes les propriétés et de les envoyer au serveur Logiciel.
- Certains programmes d'installation peuvent nécessiter un accès à la console tty. Redirigez les entrées à partir de `/dev/console`. Par exemple, un composant Logiciel RabbitMQ peut utiliser la commande `./rabbitmq_rhel.py --setup-rabbitmq < /dev/console` dans son script d'installation.
- Lorsqu'un composant utilise plusieurs étapes de cycle de vie, la valeur de la propriété peut être modifiée dans l'étape de cycle de vie INSTALLATION. La nouvelle valeur est envoyée à la prochaine étape de cycle de vie. Les scripts d'action peuvent calculer la valeur d'une propriété au cours du déploiement, afin de fournir la valeur à d'autres scripts dépendants. Par exemple, dans l'exemple d'application Clustered Dukes Bank, le service JBossAppServer calcule la propriété JVM_ROUTE au cours de l'étape de cycle de vie INSTALLATION. Cette propriété est utilisée par le service JBossAppServer pour configurer le cycle de vie. Le service d'équilibrage de charge Apache lie ensuite sa propriété JVM_ROUTE à la propriété `all(appserver:JbossAppServer:JVM_ROUTE)` pour obtenir la valeur calculée finale de node0 et node1. Si un composant a besoin d'une valeur de propriété d'un autre composant pour terminer le déploiement d'une application, vous devez indiquer des dépendances explicites dans le Blueprint d'application.

Remarque Vous ne pouvez pas modifier la valeur de propriété de contenu d'un composant qui utilise plusieurs étapes de cycle de vie.

Créer un composant Logiciel

Configurez et publiez un composant Logiciel que les autres architectes de logiciel, les architectes IaaS et les architectes d'application peuvent utiliser afin d'assembler les Blueprints d'application.

Prérequis

Connectez-vous à la console vRealize Automation en tant qu'**architecte de logiciel**.

Procédure

1 Sélectionnez **Conception > Composants logiciels**.

2 Cliquez sur l'icône **Ajouter** (+).

3 Entrez un nom et, éventuellement, une description.

À l'aide du nom que vous avez spécifié pour votre composant Logiciel, vRealize Automation crée un identifiant pour le composant Logiciel qui est unique au sein de votre locataire. Vous pouvez modifier ce champ maintenant, mais une fois le Blueprint enregistré, vous ne pourrez plus le modifier. Du fait que les identifiants sont permanents et uniques au sein de votre locataire, vous pouvez les utiliser pour interagir par programmation avec les Blueprints et pour créer des liaisons de propriétés.

4 (Facultatif) Pour contrôler le mode d'inclusion du composant Logiciel dans les Blueprints, sélectionnez un type de conteneur dans le menu déroulant **Conteneur**.

Option	Description
Machines	Le composant Logiciel doit être placé directement sur une machine.
Un de vos composants Logiciel publiés	Si vous concevez un composant Logiciel spécifiquement afin de l'installer sur un autre composant Logiciel que vous avez créé, sélectionnez ce composant Logiciel dans la liste. Par exemple, si vous concevez un composant EAR pour l'installer sur un composant JBOSS précédemment créé, sélectionnez ce dernier dans la liste de composants.
Composants logiciels	Si vous concevez un composant Logiciel qui ne doit pas être installé directement sur une machine mais qui peut être installé sur plusieurs composants Logiciel différents, sélectionnez l'option Composants logiciels. Par exemple, si vous concevez un composant WAR que vous souhaitez installer sur le composant Logiciel du serveur Tomcat et le composant Logiciel Tcserver, sélectionnez le type de conteneur des composants logiciels.

5 Cliquez sur **Suivant**.

6 Définissez les propriétés que vous souhaitez utiliser dans vos scripts d'action.

a Cliquez sur l'icône **Ajouter** (+).

b Entrez le nom de la propriété.

c Entrez la description de la propriété.

Cette description permet aux architectes de connaître les utilisateurs des composants Logiciel dans les Blueprints.

- d Sélectionnez le type escompté de la valeur de la propriété.
- e Définissez la valeur de la propriété.

Option	Description
Utiliser la valeur que vous venez de fournir	<ul style="list-style-type: none"> ■ Entrez une valeur. ■ Désélectionnez l'option Remplaçable. ■ Sélectionnez l'option Requis.
Obliger les architectes à fournir une valeur	<ul style="list-style-type: none"> ■ Entrez une valeur par défaut. ■ Sélectionnez l'option Remplaçable. ■ Sélectionnez l'option Requis.
Autoriser les architectes à fournir une valeur s'ils le souhaitent	<ul style="list-style-type: none"> ■ Entrez une valeur par défaut. ■ Sélectionnez l'option Remplaçable. ■ Désélectionnez l'option Requis.

Les architectes peuvent configurer les propriétés Logiciel afin qu'elles apparaissent dans le formulaire de demande des utilisateurs. Les architectes peuvent utiliser l'option Afficher dans la demande pour obliger les utilisateurs à remplir les valeurs des propriétés que vous marquez en tant que remplaçables, ou leur demander de le faire.

- 7 Suivez les invites qui s'affichent pour fournir un script à au moins une des actions du cycle de vie du logiciel.

Tableau 3-48. Actions du cycle de vie

Actions du cycle de vie	Description
Installer	Installez votre logiciel. Vous pouvez, par exemple, télécharger une installation du serveur Tomcat et installer un service Tomcat. Les scripts que vous écrivez pour l'action du cycle de vie Installer s'exécutent lorsque le logiciel est provisionné pour la première fois, soit lors d'une demande de déploiement initial, soit dans le cadre d'une montée en charge.
Configurer	Configurez votre logiciel. Dans l'exemple de Tomcat, vous pouvez définir les options JAVA_OPTS et CATALINA_OPTS. Les scripts de configuration s'exécutent une fois l'action Installer terminée.
Démarrer	Démarrez votre logiciel. Vous pouvez, par exemple, démarrer le service Tomcat à l'aide de la commande Démarrer du serveur Tomcat. Les scripts de démarrage s'exécutent une fois l'action Configurer terminée.
Mettre à jour	Si vous concevez votre composant logiciel de sorte à ce qu'il prenne en charge des Blueprints évolutifs, gérez les mises à jour requises après une opération de réduction de charge ou de montée en charge. Vous pouvez, par exemple, modifier la taille du cluster pour un déploiement dimensionné et gérer les nœuds en cluster à l'aide d'un équilibrage de charge. Concevez vos scripts de mise à jour de sorte à ce qu'ils s'exécutent plusieurs fois (idempotent) et qu'ils traitent à la fois les cas de réduction de charge et de montée en charge. Lorsqu'une opération de dimensionnement est effectuée, les scripts de mise à jour s'exécutent sur tous les composants logiciels dépendants.
Désinstaller	Désinstallez votre logiciel. Vous pouvez, par exemple, effectuer des actions spécifiques dans l'application avant la destruction d'un déploiement. Les scripts de désinstallation s'exécutent chaque fois que des composants logiciels sont détruits.

Entrez des codes d'état et de sortie dans vos scripts d'action. Chaque type de script pris en charge possède des conditions uniques relatives à son code d'état et de sortie.

Type de script	État de réussite	État d'erreur	Commandes non prises en charge
Bash	<ul style="list-style-type: none"> ■ return 0 ■ exit 0 	<ul style="list-style-type: none"> ■ return non-zero ■ exit non-zero 	Aucun
Windows CMD	exit /b 0	exit /b non-zero	N'utilisez pas les codes exit 0 et exit non-zero.
PowerShell	exit 0	exit non-zero;	N'utilisez pas les appels warning, verbose, debug et host.

- 8 Cochez la case **Redémarrer** pour tous les scripts qui vous obligent à redémarrer la machine.
Après l'exécution du script, la machine redémarre avant de lancer le prochain script de cycle de vie.
- 9 Cliquez sur **Terminer**.
- 10 Sélectionnez votre composant Logiciel et cliquez sur **Publier**.

Vous avez configuré et publié un composant Logiciel. Les autres architectes de logiciel, les architectes IaaS et les architectes d'application peuvent utiliser ce composant Logiciel pour ajouter des logiciels à des Blueprints d'application.

Suivant

Ajoutez le composant Logiciel publié à un Blueprint d'application. Reportez-vous à [Assemblage de Blueprints composites](#).

Paramètres de composant Logiciel

Configurez des paramètres généraux, créez des propriétés et écrivez des scripts d'action pour installer, configurer, mettre à jour ou désinstaller votre composant Logiciel sur des machines provisionnées.

En tant qu'architecte de logiciels, cliquez sur **Conception > Composants logiciels** et cliquez sur l'icône **Ajouter** pour créer un nouveau composant Logiciel.

Nouveaux paramètres Logiciel généraux

Appliquez des paramètres généraux à votre composant Logiciel.

Tableau 3-49. Nouveaux paramètres Logiciel généraux

Configuration	Description
Nom	Entrez un nom pour votre composant Logiciel.
ID	À l'aide du nom que vous avez spécifié pour votre composant Logiciel, vRealize Automation crée un identifiant pour le composant Logiciel qui est unique au sein de votre locataire. Vous pouvez modifier ce champ maintenant, mais une fois le Blueprint enregistré, vous ne pourrez plus le modifier. Du fait que les identifiants sont permanents et uniques au sein de votre locataire, vous pouvez les utiliser pour interagir par programmation avec les Blueprints et pour créer des liaisons de propriétés.

Tableau 3-49. Nouveaux paramètres Logiciel généraux (suite)

Configuration	Description
Description	Résumez votre composant Logiciel à l'attention d'autres architectes.
Conteneur	<p>Les architectes de Blueprint peuvent uniquement placer votre composant Logiciel sur le canevas de conception dans le type de conteneur que vous sélectionnez.</p> <ul style="list-style-type: none"> ■ Sélectionnez Machines pour obliger les architectes à placer votre composant Logiciel directement sur un composant de machine sur le canevas de conception. ■ Sélectionnez Composants logiciels si vous concevez un composant Logiciel qui ne doit jamais être placé directement sur un composant de machine, mais qui peut être imbriqué dans l'un des différents composants Logiciel. ■ Sélectionnez un composant Logiciel publié spécifique si vous concevez un composant Logiciel qui doit spécifiquement être imbriqué dans un autre composant Logiciel que vous avez créé. ■ Sélectionnez la machine virtuelle Azure si vous concevez un composant Logiciel spécifiquement pour un Blueprint Azure.

Nouvelles propriétés Logiciel

Les propriétés de composant Logiciel sont utilisées pour paramétrer les scripts afin de transmettre les propriétés définies comme des variables d'environnement aux scripts s'exécutant sur une machine virtuelle. Avant d'exécuter vos scripts, l'agent Logiciel de la machine provisionnée communique avec vRealize Automation pour résoudre les propriétés. Ensuite, l'agent crée des variables propres au script à partir de ces propriétés et les transmet aux scripts.

Tableau 3-50. Nouvelles propriétés Logiciel

Configuration	Description
Nom	Entrez un nom pour votre propriété Logiciel. Les noms des propriétés sont sensibles à la casse et ne peuvent contenir que des caractères alphabétiques, numériques, de soulignement (_), ou des traits d'union (-).
Description	Résumez votre propriété et toutes les conditions requises de la valeur à l'attention d'autres utilisateurs.
Type	Logiciel prend en charge les types suivants : chaîne, groupe, contenu, booléen et entier. Pour obtenir une explication détaillée des types de propriétés pris en charge, reportez-vous à Types de propriétés et options de paramètres . Pour plus d'informations sur les liaisons de propriétés, reportez-vous à Cas où votre composant Logiciel doit utiliser les informations d'un autre composant et Création de liaisons de propriétés entre des composants de Blueprint .

Tableau 3-50. Nouvelles propriétés Logiciel (suite)

Configuration	Description
Valeur	<ul style="list-style-type: none"> ■ Pour utiliser la valeur que vous avez fournie : <ul style="list-style-type: none"> ■ Entrez une valeur. ■ Sélectionnez l'option Requis. ■ Désélectionnez l'option Remplaçable. ■ Pour obliger les architectes à fournir une valeur : <ul style="list-style-type: none"> ■ (Facultatif) Entrez une valeur comme valeur par défaut. ■ Sélectionnez l'option Remplaçable. ■ Sélectionnez l'option Requis. ■ Pour autoriser les architectes à fournir une valeur ou laisser la zone vide : <ul style="list-style-type: none"> ■ (Facultatif) Entrez une valeur comme valeur par défaut. ■ Sélectionnez l'option Remplaçable. ■ Désélectionnez l'option Requis.
Chiffré	<p>Marquez les propriétés comme chiffrées afin de masquer la valeur et de la remplacer par des astérisques dans vRealize Automation. Si vous passez une propriété de chiffrée à non chiffrée, vRealize Automation réinitialise la valeur de la propriété. À des fins de sécurité, vous devez définir une nouvelle valeur pour la propriété.</p> <p>Important Si des propriétés sécurisées sont écrites dans le script à l'aide de la commande echo ou d'autres commandes semblables, ces valeurs s'affichent en texte clair dans les fichiers journaux. Les valeurs figurant dans les fichiers journaux ne sont pas masquées.</p>
Remplaçable	Autorisez les architectes à modifier la valeur de cette propriété lorsqu'ils assemblent un Blueprint d'application. Si vous entrez une valeur, elle s'affiche en tant que valeur par défaut.
Obligatoire	Obligez les architectes à fournir une valeur pour cette propriété ou à accepter la valeur par défaut que vous fournissez.
Calculée	Les valeurs des propriétés calculées sont attribuées par les scripts de cycle de vie INSTALLATION, CONFIGURATION, DÉMARRAGE ou MISE À JOUR. La valeur attribuée est propagée aux étapes disponibles suivantes du cycle de vie et aux composants qui sont liés à ces propriétés dans un Blueprint. Si vous sélectionnez la valeur Calculée pour une propriété qui n'est pas une propriété de type chaîne, le type de propriété est changé en chaîne.

Nouvelles actions Logiciel

Vous créez des scripts d'action Bash, Windows CMD ou PowerShell pour spécifier comment les composants sont installés, configurés, désinstallés ou mis à jour lors des opérations de dimensionnement de déploiement.

Tableau 3-51. Actions du cycle de vie

Actions du cycle de vie	Description
Installer	Installez votre logiciel. Vous pouvez, par exemple, télécharger une installation du serveur Tomcat et installer un service Tomcat. Les scripts que vous écrivez pour l'action du cycle de vie Installer s'exécutent lorsque le logiciel est provisionné pour la première fois, soit lors d'une demande de déploiement initial, soit dans le cadre d'une montée en charge.
Configurer	Configurez votre logiciel. Dans l'exemple de Tomcat, vous pouvez définir les options JAVA_OPTS et CATALINA_OPTS. Les scripts de configuration s'exécutent une fois l'action Installer terminée.
Démarrer	Démarrez votre logiciel. Vous pouvez, par exemple, démarrer le service Tomcat à l'aide de la commande Démarrer du serveur Tomcat. Les scripts de démarrage s'exécutent une fois l'action Configurer terminée.
Mettre à jour	Si vous concevez votre composant logiciel de sorte à ce qu'il prenne en charge des Blueprints évolutifs, gérez les mises à jour requises après une opération de réduction de charge ou de montée en charge. Vous pouvez, par exemple, modifier la taille du cluster pour un déploiement dimensionné et gérer les nœuds en cluster à l'aide d'un équilibrage de charge. Concevez vos scripts de mise à jour de sorte à ce qu'ils s'exécutent plusieurs fois (idempotent) et qu'ils traitent à la fois les cas de réduction de charge et de montée en charge. Lorsqu'une opération de dimensionnement est effectuée, les scripts de mise à jour s'exécutent sur tous les composants logiciels dépendants.
Désinstaller	Désinstallez votre logiciel. Vous pouvez, par exemple, effectuer des actions spécifiques dans l'application avant la destruction d'un déploiement. Les scripts de désinstallation s'exécutent chaque fois que des composants logiciels sont détruits.

Cochez la case **Redémarrer** pour tous les scripts qui vous obligent à redémarrer la machine. Après l'exécution du script, la machine redémarre avant de lancer le prochain script de cycle de vie. Vérifiez qu'aucun processus n'invite l'utilisateur à interagir lorsque le script d'action est en cours d'exécution. Les interruptions suspendent le script, le plaçant dans un état d'inactivité indéfini, pour finir par le faire échouer. De plus, vos scripts doivent inclure des codes exit adéquats, qui s'appliquent au déploiement de l'application. Si le script ne comporte pas de codes exit et return, la dernière commande exécutée dans le script devient l'état de sortie. Les codes exit et return varient selon les types de scripts pris en charge (Bash, Windows CMD, PowerShell).

Type de script	État de réussite	État d'erreur	Commandes non prises en charge
Bash	<ul style="list-style-type: none"> ■ return 0 ■ exit 0 	<ul style="list-style-type: none"> ■ return non-zero ■ exit non-zero 	Aucun
Windows CMD	exit /b 0	exit /b non-zero	N'utilisez pas les codes exit 0 et exit non-zero.
PowerShell	exit 0	exit non-zero;	N'utilisez pas les appels warning, verbose, debug et host.

Conception de Blueprints XaaS et d'actions sur les ressources

Vous pouvez publier les Blueprints XaaS en tant qu'éléments du catalogue ou les utiliser dans le canevas de conception de Blueprints. Les actions sur les ressources sont des actions que vous exécutez sur des éléments déployés.

XaaS utilise vRealize Orchestrator pour exécuter des workflows qui provisionnent les éléments ou pour exécuter des actions. Par exemple, vous pouvez configurer les workflows afin de créer des machines virtuelles vSphere, des utilisateurs Active Directory dans des groupes ou pour exécuter des scripts PowerShell. Si vous créez un workflow vRealize Orchestrator personnalisé, vous pouvez fournir ce workflow en tant qu'élément du catalogue de services afin que les utilisateurs autorisés puissent exécuter le workflow.

Vous pouvez utiliser un Blueprint XaaS en tant que composant d'un Blueprint que vous créez dans le canevas de conception ou le publier directement dans le catalogues de services.

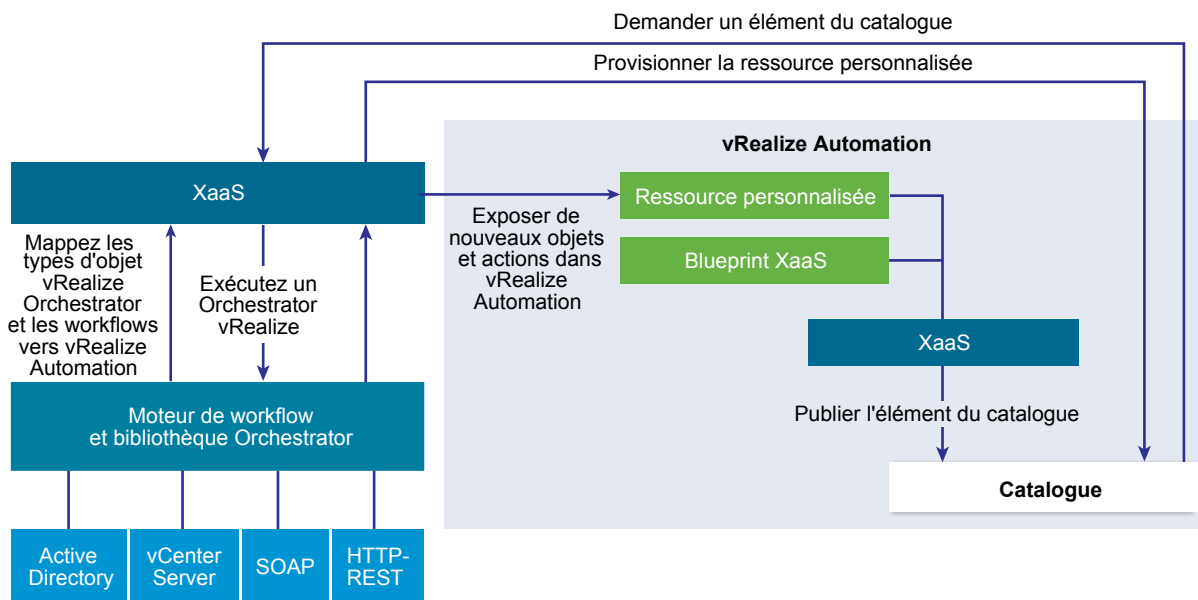
Si vous utilisez un Blueprint en tant que composant dans un autre Blueprint, vous pouvez le configurer pour l'adapter lors d'une action de réduction de charge ou de montée en charge.

Intégration de vRealize Orchestrator dans vRealize Automation

vRealize Orchestrator est le moteur de workflow intégré à vRealize Automation

Le serveur vRealize Orchestrator distribué avec vRealize Automation est préconfiguré et, par conséquent, lorsque votre administrateur système déploie le dispositif vRealize Automation, le serveur vRealize Orchestrator est en cours d'exécution.

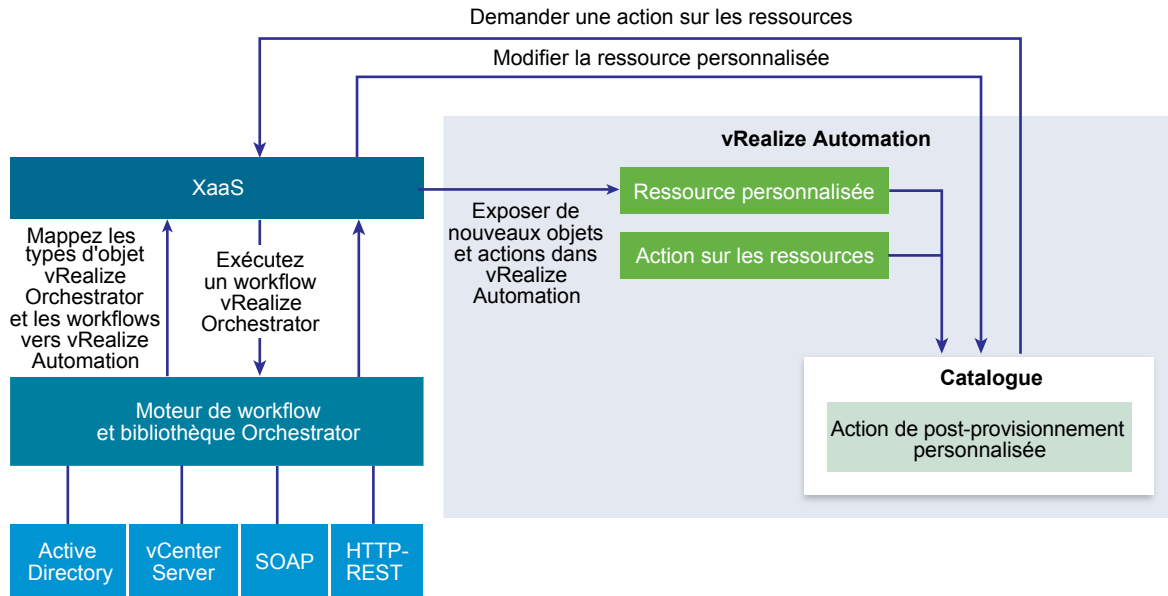
Figure 3-2. Création et demande d'éléments de catalogue inclus dans une solution XaaS pour provisionner une ressource personnalisée



Les architectes de services XaaS ajoutent des ressources personnalisées associées aux points de terminaison pris en charge et fournissent des workflows, puis créent des Blueprints et actions XaaS basés sur ces ressources. Les administrateurs de locataire et les gestionnaires de groupes d'activité peuvent ajouter les Blueprints et actions XaaS au catalogue de services. Le Blueprint XaaS peut également être utilisé dans le concepteur de Blueprint.

Lorsque l'utilisateur d'un catalogue de services demande un élément, vRealize Automation exécute un workflow vRealize Orchestrator pour provisionner la ressource personnalisée.

Figure 3-3. Création et demande d'actions sur les ressources personnalisées pour modifier une ressource personnalisée



Les architectes de solutions XaaS peuvent également ajouter des workflows vRealize Orchestrator en tant qu'actions sur les ressources afin d'étendre les capacités de vRealize Automation. Une fois que les utilisateurs du catalogue de services ont provisionné une ressource personnalisée, ils peuvent exécuter une action de post-provisionnement. Les consommateurs exécutent ainsi un workflow vRealize Orchestrator et modifient la ressource personnalisée provisionnée.

Lorsqu'un utilisateur du catalogue de services demande une action sur les Blueprint ou sur les ressources XaaS en tant qu'élément de catalogue, le service XaaS exécute le workflow vRealize Orchestrator correspondant en transférant les données suivantes en tant que paramètres globaux au workflow :

Tableau 3-52. Paramètres globaux XaaS

Paramètre	Description
__asd_tenantRef	Le locataire de l'utilisateur ayant demandé le workflow.
__asd_subtenantRef	Le groupe d'activité de l'utilisateur ayant demandé le workflow.
__asd_catalogRequestId	L'identifiant de la demande du catalogue pour l'exécution de ce workflow.
__asd_requestedFor	L'utilisateur cible de la demande. Si la demande est faite au nom d'un utilisateur, il s'agit de l'utilisateur au nom duquel le workflow est demandé, sinon, il s'agit de l'utilisateur ayant demandé le workflow.
__asd_requestedBy	L'utilisateur ayant demandé le workflow.

Si une action sur les Blueprints ou sur les ressources XaaS utilise un workflow vRealize Orchestrator qui contient un élément du schéma de l'interaction utilisateur, lorsqu'un consommateur demande le service, le workflow suspend son exécution et attend que l'utilisateur fournisse les données requises. Pour répondre à une interaction utilisateur en attente, l'utilisateur doit accéder à **Boîte de réception > Action Manuelle de l'Utilisateur**.

Le répertoire du serveur vRealize Orchestrator par défaut est partagé par tous les locataires et son utilisation ne peut pas se faire individuellement par utilisateur. Par exemple, si un architecte de service crée un Blueprint de service pour créer une ressource de calcul du cluster, les consommateurs de différents locataires doivent accéder aux éléments du répertoire de toutes les instances de vCenter Server même si elles appartiennent à un locataire différent.

Les administrateurs système peuvent installer vRealize Orchestrator ou déployer le dispositif vRealize Orchestrator Appliance séparément pour configurer une instance externe de vRealize Orchestrator et configurer vRealize Automation pour l'utiliser avec cette instance externe de vRealize Orchestrator.

Les administrateurs système peuvent également configurer des catégories de workflows vRealize Orchestrator par locataire et définir quels workflows seront disponibles pour chaque locataire.

De plus, les administrateurs de locataire peuvent également configurer une instance externe de vRealize Orchestrator mais uniquement pour leurs propres locataires.

Pour plus d'informations sur la configuration d'une instance externe de vRealize Orchestrator et des catégories de workflow vRealize Orchestrator, reportez-vous à *Configuration de vCenter Orchestrator et des plug-ins*.

Liste des plug-ins vRealize Orchestrator

Avec des plug-ins, vous pouvez utiliser vRealize Orchestrator pour accéder et contrôler des technologies et des applications externes. En exposant une technologie externe dans un plug-in vRealize Orchestrator, vous pouvez incorporer des objets et des fonctions aux workflows qui accèdent aux objets et aux fonctions de cette technologie externe.

Les technologies externes auxquelles vous pouvez accéder en utilisant des plug-ins peuvent inclure des outils de gestion de virtualisation, des systèmes de messagerie, des bases de données, des services d'annuaire, des interfaces de contrôle à distance, etc.

Vous pouvez utiliser l'ensemble standard de plug-ins vRealize Orchestrator pour incorporer des technologies externes telles que l'API vCenter Server et les fonctions de messagerie aux workflows. Vous pouvez également utiliser l'architecture modulaire ouverte de vRealize Orchestrator pour développer des plug-ins afin d'accéder à d'autres applications.

Tableau 3-53. Plug-ins inclus par défaut dans vRealize Orchestrator

Plug-in	Objectif
vCenter Server	Fournir un accès à l'API vCenter Server de sorte à pouvoir incorporer l'ensemble des objets et des fonctions vCenter Server aux processus de gestion que vous automatisez à l'aide de vRealize Orchestrator.
Configuration	Fournit des workflows permettant de configurer l'authentification de vRealize Orchestrator, la connexion de la base de données, des certificats SSL, etc.
Bibliothèque vCO	Fournit des workflows qui agissent tels des composants de base pour la personnalisation et l'automatisation des processus client. La bibliothèque de workflows inclut des modèles pour la gestion du cycle de vie, le provisionnement, la récupération d'urgence, la sauvegarde à chaud et d'autres processus standard. Vous pouvez copier et modifier les modèles pour les adapter à vos besoins.
SQL	Fournit l'API Java Database Connectivity (JDBC), qui constitue la norme de l'industrie pour une connectivité indépendante de la base de données entre le langage de programmation Java et de nombreuses bases de données. Les bases de données incluent des bases de données SQL et d'autres sources de données tabulaires, comme des feuilles de calcul ou des fichiers plats. L'API JDBC fournit une API de niveau appel pour l'accès aux bases de données SQL depuis les workflows.
SSH	Fournit une implémentation du protocole Secure Shell v2 (SSH-2). Permet des sessions de commande à distance et de transfert de fichiers avec authentification par mot de passe et clé publique dans les workflows. Prend en charge l'authentification par clavier interactif. Le plug-in SSH peut fournir une exploration à distance du système de fichiers directement dans l'inventaire client vRealize Orchestrator.
XML	Un analyseur XML complet de modèle d'objet de documents (DOM) XML que vous pouvez implémenter dans les workflows. Vous pouvez également utiliser l'implémentation ECMAScript for XML (E4X) dans l'API JavaScript de vRealize Orchestrator.
Mail	Utilise le protocole SMTP (Simple Mail Transfer Protocol) pour envoyer des e-mails depuis les workflows.
Net	Renvoie la bibliothèque Jakarta Apache Commons Net. Fournit des implémentations de Telnet, FTP, POP3 et IMAP. La partie POP3 et IMAP est utilisée pour lire les e-mails. Associé au plug-in Mail, le plug-in Net fournit des fonctions complètes d'envoi et de réception d'e-mails dans les workflows.
Énumération	Fournit des types énumérés communs qui peuvent être utilisés dans les workflows par d'autres plug-ins.
Documentation sur les workflows	Fournit des workflows qui vous permettent de générer des informations au format PDF concernant un workflow ou une catégorie de workflows.
HTTP-REST	Vous permet de gérer des services Web REST en fournissant une interaction entre les hôtes vCenter Orchestrator et REST.
SOAP	Vous permet de gérer des services Web SOAP en fournissant une interaction entre les hôtes vCenter Orchestrator et SOAP.
AMQP	Vous permet d'interagir avec les serveurs Advanced Message Queuing Protocol (AMQP), également appelés brokers.

Tableau 3-53. Plug-ins inclus par défaut dans vRealize Orchestrator (suite)

Plug-in	Objectif
SNMP	Permet à vCenter Orchestrator de se connecter et de recevoir des informations provenant des systèmes et périphériques SNMP.
Active Directory	Fournit une interaction entre vCenter Orchestrator et Microsoft Active Directory.
vCO WebOperator	Une vue Web qui vous permet d'accéder aux workflows de la bibliothèque vRealize Orchestrator et d'interagir avec eux sur un réseau en utilisant un navigateur Web.
Types dynamiques	Vous permet de définir des types dynamiques et de créer et d'utiliser des objets de ces types dynamiques.
PowerShell	Vous permet de gérer des hôtes PowerShell et d'exécuter des opérations PowerShell personnalisées.
Nœuds multiples	Contient des workflows pour une orchestration hiérarchique, la gestion des instances Orchestrator et la montée en charge des activités Orchestrator.
vRealize Automation	Vous permet de créer et d'exécuter des workflows pour l'interaction entre vRealize Orchestrator et vRealize Automation.

Pour plus d'informations sur les plug-ins vRealize Orchestrator que VMware développe et distribue, reportez-vous à la page de destination de la documentation VMware vRealize™ Orchestrator™.

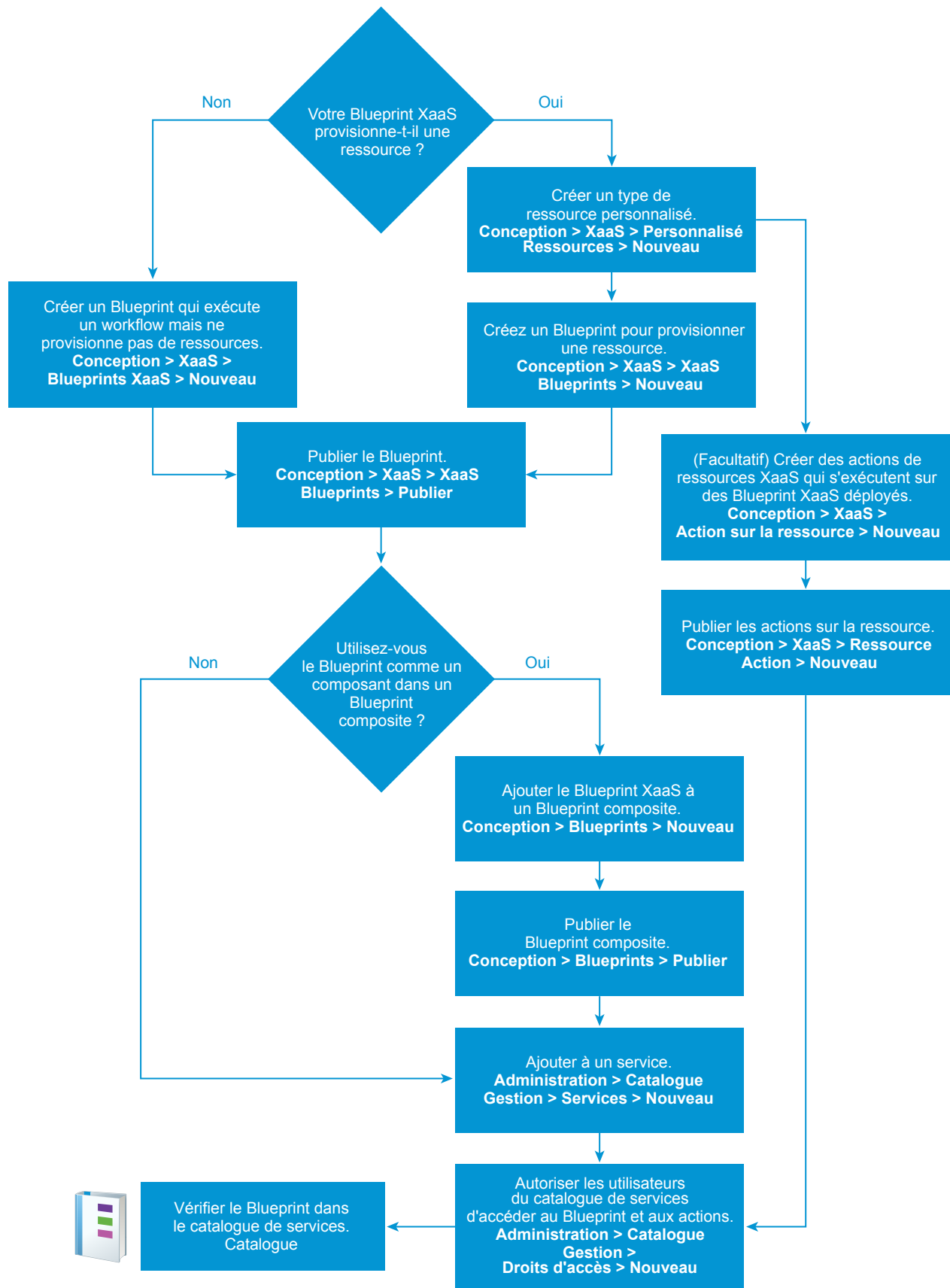
Création de Blueprints XaaS et d'actions sur les ressources

Les Blueprints XaaS peuvent être mis à la disposition d'utilisateurs en tant qu'éléments du catalogue. Ils peuvent aussi être assemblés en Blueprints composites à l'aide du canevas de conception. Les actions sur les ressources sont exécutées sur les éléments provisionnés, afin de les gérer après leur provisionnement.

Par exemple, vous pouvez utiliser un Blueprint XaaS afin de créer des utilisateurs Active Directory dans un groupe. Vous pouvez ensuite utiliser une action sur la ressource pour exiger que l'utilisateur change son mot de passe.

Workflow de Blueprint XaaS

Le workflow que vous suivez pour créer un Blueprint XaaS et les actions sur les ressources facultatives dépendent de la manière dont vous prévoyez d'utiliser le Blueprint. Le workflow suivant fournit le processus de base.



Terminologie des Blueprints XaaS

Les Blueprints XaaS sont des workflows vRealize Orchestrator pouvant provisionner des ressources, modifier les ressources provisionnées ou se comporter comme un service effectuant une tâche dans votre environnement. Les Blueprints et les actions sur les ressources ont différentes nuances que vous devez comprendre lorsque vous concevez des Blueprints pour les utilisateurs de votre catalogue de services.

Les définitions suivantes vous permettent de comprendre les termes utilisés lorsque vous travaillez avec des Blueprints XaaS.

Ressource personnalisée	Type d'objet vRealize Orchestrator exposé en tant que ressource par le biais de l'API d'un plug-in vRealize Orchestrator. Vous créez une ressource personnalisée pour définir le paramètre de sortie d'un Blueprint de provisionnement XaaS et pour définir un paramètre d'entrée d'une action sur la ressource.
Composant de Blueprint XaaS	Blueprint de provisionnement ou de non-provisionnement que vous pouvez utiliser dans le canevas de conception du Blueprint. Ce Blueprint peut également être un Blueprint XaaS autonome.
Blueprint XaaS autonome	Blueprint de provisionnement ou de non-provisionnement qui est publié et autorisé directement dans le catalogue de services.
Blueprint de provisionnement	<p>Blueprint de provisionnement qui exécute un workflow vRealize Orchestrator pour provisionner des ressources sur le point de terminaison cible à l'aide de l'API de plug-in vRealize Orchestrator pour le point de terminaison. Par exemple, ajoutez des cartes réseau virtuelles à un périphérique réseau dans vSphere. Pour créer un Blueprint de provisionnement, vous devez disposer d'une ressource personnalisée qui définit le type de ressource vRealize Orchestrator.</p> <p>Lorsqu'un utilisateur du catalogue de services demande ce type d'éléments du catalogue, le workflow provisionne l'élément et l'élément déployé est stocké sur l'onglet Éléments. Vous pouvez définir des opérations de post-provisionnement sur ce type de ressources provisionnées. Vous pouvez également rendre les Blueprints évolutifs en ajoutant ou supprimant une instance, le cas échéant.</p>
Blueprint de non-provisionnement	<p>Un Blueprint de non-provisionnement exécute un workflow vRealize Orchestrator pour effectuer une tâche qui ne nécessite pas que l'API apporte des modifications au point de terminaison. Par exemple, le workflow qui s'exécute crée un rapport puis l'envoie par e-mail ou le publie sur le système de communication cible.</p> <p>Lorsqu'un utilisateur du catalogue de services demande ce type d'élément du catalogue, le workflow s'exécute pour effectuer la tâche du script, mais l'élément n'est pas ajouté sur l'onglet Éléments. Il est impossible d'exécuter des opérations de post-provisionnement sur ce type de</p>

Blueprint. Vous pouvez utiliser des Blueprints de non-provisionnement comme workflows de prise en charge dans des Blueprints évolutifs. Par exemple, vous pouvez créer un Blueprint pour mettre à jour un équilibrage de charge à haute disponibilité.

Blueprint composite

Blueprint qui a été créé à l'aide du canevas de conception. Le Blueprint composite utilise un ou plusieurs composants. Par exemple, un composant de machine, un composant logiciel ou un composant XaaS. Lorsque vous l'ajoutez à un service, il est répertorié comme un Déploiement. Lorsque vous l'ajoutez à un droit pour le mettre à la disposition des utilisateurs du catalogue de services, il est répertorié comme un Blueprint composite. Un Blueprint composite peut comporter un composant de Blueprint ou inclure l'intégralité d'une application avec plusieurs machines, logiciels et mises en réseau.

Action sur la ressource

Workflow que vous pouvez exécuter sur un Blueprint de provisionnement déployé. Le Blueprint déployé peut être un Blueprint ou un composant de Blueprint XaaS, ou un type de machine que vous avez mappé à un type de ressource vRealize Orchestrator.

Considérations relatives à la conception de Blueprints XaaS

Avant de créer un Blueprint XaaS, vous devez comprendre son objectif afin de créer celui qui provisionne correctement vos ressources.

Vous pouvez créer et utiliser des Blueprints XaaS comme composant de Blueprint dans le canevas de conception ou en tant que Blueprint autonome. Le Blueprint peut être un Blueprint de provisionnement ou non.

Tableau 3-54. Types de Blueprint XaaS et résultats

Type de Blueprint XaaS	Une ressource personnalisée est-elle nécessaire ?	Le Blueprint est-il évolutif dans un déploiement ?	Est-ce que je peux exécuter une action sur la ressource sur le Blueprint déployé ?
Composant de Blueprint provisionnant des ressources	Oui	Oui. Configuré pour le dimensionnement, et dimensionné en même temps que le déploiement.	Oui. Dimensionné en même temps que le déploiement, et vous pouvez exécuter d'autres actions sur les ressources sur le composant déployé. Le composant de Blueprint s'affiche sur votre onglet Éléments.
Composant de Blueprint exécutant un workflow mais ne provisionnant pas de ressources	Non. Le Blueprint utilise la configuration de serveur vRealize Orchestrator, mais ne nécessite pas de ressource personnalisée XaaS.	Non. Provisionne les ressources, mais peut s'exécuter dans le cadre d'une opération de dimensionnement. Par exemple, mettez à jour un équilibrage de charge avec la nouvelle configuration basée sur l'opération de dimensionnement.	Non. Vous ne pouvez pas exécuter d'action sur la ressource sur un composant qui n'est pas un composant de dimensionnement.
Blueprint autonome provisionnant des ressources	Oui	Non. Vous devez créer des actions sur les ressources pour ajouter ou détruire des instances.	Oui. Vous pouvez exécuter des actions sur la ressource déployée, y compris des actions que vous avez créées pour prendre en charge le dimensionnement. Le Blueprint s'affiche sur votre onglet Éléments.
Blueprint autonome exécutant un workflow mais ne provisionnant pas de ressources	Non. Le Blueprint utilise la configuration de serveur vRealize Orchestrator, mais ne nécessite pas de ressource personnalisée XaaS.	Non. Ne provisionne pas les ressources, mais peut s'exécuter dans le cadre d'une action sur la ressource.	Non. Vous ne pouvez pas exécuter d'action sur la ressource sur un composant qui n'est pas un composant de dimensionnement.

Ajouter une ressource personnalisée XaaS

Créez une ressource personnalisée pour définir l'élément XaaS à des fins de provisionnement. Avant de créer un Blueprint ou une action XaaS, vous devez disposer d'une ressource personnalisée qui est compatible avec le type d'objet du workflow de Blueprint ou d'action.

En créant une ressource personnalisée, mappez un type d'objet exposé par l'API d'un plug-in vRealize Orchestrator en tant que ressource. La ressource personnalisée définit le paramètre de sortie d'un Blueprint XaaS pour le provisionnement et un paramètre d'entrée d'une action sur la ressource.

Si un workflow de Blueprint ou d'action sur la ressource ne provisionne pas une ressource ou n'est pas exécuté sur un Blueprint déployé, il n'est pas nécessaire de créer une ressource personnalisée. Par exemple, vous n'avez pas besoin de ressource personnalisée si votre workflow met à jour une valeur de base de données ou envoie un message électronique après une opération de provisionnement.

Lorsque vous créez une ressource personnalisée, vous pouvez spécifier les champs du formulaire en lecture seule relatifs aux détails d'un élément provisionné. Reportez-vous à [Conception d'un formulaire de ressource personnalisée](#).

Prérequis

- Connectez-vous à la console vRealize Automation en tant qu'**architecte XaaS**.
- Pour configurer la ressource personnalisée, utilisez les informations des options détaillées. Reportez-vous à [Options de l'assistant Ressource personnalisée XaaS](#).

Procédure

- 1 Sélectionnez **Conception > XaaS > Ressources personnalisées**.
- 2 Cliquez sur l'icône **Nouveau** (+).
- 3 Configurez les valeurs dans l'onglet **Type de ressource**.
 - a Entrez ou sélectionnez le type d'objet vRealize Orchestrator dans la zone de texte **Type de la variable dans l'orchestrateur**.
 Par exemple, entrez **v** pour afficher les types contenant la lettre v. Pour afficher tous les types, entrez un espace.
 - b Entrez un nom et, éventuellement, une description.
 - c Entrez une version.
 Le format pris en charge couvre les version-majeure.version-mineure.micro-version.
 - d Cliquez sur **Suivant**.
- 4 Entrez les valeurs requises dans l'onglet **Formulaire de détails**.
 Vous pouvez modifier le formulaire de la ressource personnalisée en supprimant, en modifiant et en réorganisant les éléments. Vous pouvez également ajouter un formulaire et des pages de formulaire, et faire glisser les éléments vers le nouveau formulaire et la nouvelle page de formulaire.
- 5 Cliquez sur **Terminer**.

Vous avez créé une ressource personnalisée qui s'affiche sur la page Ressources personnalisées. Vous pouvez créer des Blueprints ou actions XaaS basés sur cette ressource personnalisée.

Suivant

- Créez un Blueprint XaaS. Reportez-vous à [Ajouter un Blueprint XaaS](#).
- Créez une action sur les ressources XaaS. Reportez-vous à [Créer une action sur la ressource XaaS](#).

Options de l'assistant Ressource personnalisée XaaS

Vous pouvez utiliser ces options de ressource personnalisée pour créer ou modifier une ressource personnalisée afin de pouvoir exécuter des workflows de Blueprint et d'action sur la ressource XaaS qui provisionnent les ressources ou modifient les ressources provisionnées.

Vous ne pouvez créer qu'une seule ressource personnalisée par type d'objet. Vous pouvez utiliser la ressource personnalisée pour plusieurs Blueprints et actions sur les ressources.

Pour créer une action sur la ressource personnalisée, sélectionnez **Conception > XaaS > Ressources personnalisées**

Type de ressource

Liste des types d'objets qui peuvent s'afficher sur l'onglet **Type de ressource** en fonction des plug-ins installés dans l'instance de vRealize Orchestrator configurée. vRealize Automation collecte les valeurs de l'instance de vRealize Orchestrator configurée.

Tableau 3-55. Options de type de ressource

Option	Description
Type de la variable dans l'orchestrateur	Entrez ou sélectionnez le type qui prend en charge le workflow que vous utilisez pour le provisionnement. Le type est composé du nom du plug-in tel qu'il apparaît dans l'API de script, par exemple VC pour vCenter, et le type d'objet, par exemple MachineVirtuelle. Dans cet exemple, l'API utilise la valeur VC:VirtualMachine. Ce type peut être le paramètre de sortie du workflow de Blueprint ou le paramètre d'entrée du workflow d'action sur la ressource.
Nom	Entrez un nom informatif pour la ressource personnalisée afin de pouvoir l'identifier lorsque vous créez des Blueprints ou des actions sur les ressources XaaS.
Description	Entrez une description détaillée.
Version	Le formulaire pris en charge couvre les version-majeure.version-mineure.micro-version.

Formulaire de détails

Les champs de ce formulaire s'affichent comme des valeurs en lecture seule lorsque les utilisateurs de votre catalogue de services provisionnent un élément qui utilise cette ressource personnalisée. Vous pouvez modifier les champs existants et ajouter de nouveaux champs définis en externe.

Pour plus d'informations sur la configuration des formulaires, reportez-vous à [Conception d'un formulaire de ressource personnalisée](#).

Cas d'utilisation

Comme vous ne pouvez créer qu'une ressource personnalisée par type d'objet, vous pouvez utiliser cette page de l'assistant pour comprendre comment la ressource personnalisée est utilisée.

Cet onglet est disponible pour les ressources personnalisées enregistrées, pas lorsque vous créez la ressource.

Tableau 3-56. Options de cas d'utilisation

Option	Description
Blueprints XaaS	<p>Liste des Blueprints configurés pour utiliser cette ressource personnalisée.</p> <p>Sur cette page, vous pouvez effectuer les actions suivantes :</p> <ul style="list-style-type: none"> ■ Modifier. Ouvre le Blueprint afin que vous puissiez voir comment il est configuré ou pour le modifier. ■ Publier/Annuler la publication. Permet de modifier l'état du Blueprint en le rendant disponible pour être utilisé dans un Blueprint composite ou pour l'ajouter à un service. Si vous annulez la publication d'un Blueprint, vous risquez de le rendre indisponible pour être utilisé dans des Blueprints composites, l'ajouter à un service ou le rendre indisponible dans le catalogue de services. ■ Supprimer. Permet de supprimer ce Blueprint du système.
Actions sur les ressources	<p>Liste des actions sur les ressources configurées pour utiliser cette ressource personnalisée.</p> <p>Sur cette page, vous pouvez effectuer les actions suivantes :</p> <ul style="list-style-type: none"> ■ Modifier. Ouvre l'action sur la ressource afin que vous puissiez voir comment elle est configurée ou pour la modifier. ■ Publier/Annuler la publication. Permet de modifier l'état de l'action sur la ressource en la rendant disponible dans un droit d'accès. Si vous annulez la publication d'une action sur la ressource, vous risquez de la rendre indisponible pour l'ajouter à un service ou pour l'exécuter sur des Blueprints déployés. ■ Supprimer. Permet de supprimer cette action sur la ressource du système.

Créer un Blueprint XaaS

Un Blueprint XaaS est un Blueprint de provisionnement ou de non provisionnement. Certains workflows de provisionnement vRealize Orchestrator fournis incluent la création de machines virtuelles, l'ajout d'utilisateurs à Active Directory ou la prise de snapshots d'une machine virtuelle. Certains workflows de non provisionnement peuvent inclure la mise à jour de l'équilibrage de charge ou la génération d'un rapport et son envoi aux destinataires.

Vous pouvez créer des Blueprints XaaS sur la base de workflows fournis dans vRealize Orchestrator, ou vous pouvez utiliser les workflows que vous créez pour atteindre des objectifs propres à votre environnement.

Procédure

1 Ajouter un Blueprint XaaS

Un Blueprint XaaS est une spécification permettant d'exécuter un workflow vRealize Orchestrator modifiant un système cible dans votre environnement. Le Blueprint inclut le workflow ; mais il peut également inclure les paramètres d'entrée, les formulaires d'envoi et en lecture seule, la séquence d'actions, ainsi que les opérations de provisionnement ou non-provisionnement.

2 Ajouter un Blueprint XaaS à un Blueprint composite

Vous ajoutez un Blueprint XaaS en tant que composant d'un Blueprint composite en suivant une procédure similaire à celle de l'ajout de composants de Blueprint dans le canevas de conception.

Ajouter un Blueprint XaaS

Un Blueprint XaaS est une spécification permettant d'exécuter un workflow vRealize Orchestrator modifiant un système cible dans votre environnement. Le Blueprint inclut le workflow ; mais il peut également inclure les paramètres d'entrée, les formulaires d'envoi et en lecture seule, la séquence d'actions, ainsi que les opérations de provisionnement ou non-provisionnement.

Vous pouvez créer des Blueprints XaaS à utiliser d'une ou plusieurs des façons suivantes :

- Créez un composant de Blueprint XaaS. Un Blueprint de composant est un Blueprint de provisionnement ou non-provisionnement que vous pouvez utiliser dans le canevas de conception dans le cadre d'un Blueprint composite. Si vous l'utilisez en tant que composant, vous devez configurer les options de cycle de vie du composant qui prennent en charge les opérations de réduction/montée en charge dans le Blueprint composite déployé.

Ce type de Blueprint peut également être publié en tant que Blueprint autonome.

- Créez un Blueprint XaaS autonome. Un Blueprint autonome est un Blueprint de provisionnement ou non-provisionnement qui est publié et autorisé directement dans le catalogue de services.

Pour consulter un exemple de création d'utilisateurs d'Active Directory exploitant un Blueprint XaaS, reportez-vous à [Créer un Blueprint XaaS ainsi qu'une action visant à créer et à modifier un utilisateur](#).

Prérequis

- Connectez-vous à la console vRealize Automation en tant qu'**architecte XaaS**.
- Si le Blueprint doit provisionner des ressources, créez une ressource personnalisée correspondant au paramètre de sortie du Blueprint de service. Reportez-vous à [Ajouter une ressource personnalisée XaaS](#). S'il n'utilise pas une API de plug-in vRealize Orchestrator, vous n'avez pas besoin de configurer une ressource personnalisée.
- En créant un Blueprint XaaS, vous publiez un workflow vRealize Orchestrator en tant que Blueprint de composant potentiel ou élément de catalogue. Le Blueprint inclut un formulaire que vous pouvez modifier. Reportez-vous à [Conception d'un formulaire de Blueprint XaaS](#).
- Utilisez les informations détaillées sur les options pour configurer le Blueprint. Reportez-vous à [Options Nouveau et Modifier de l'assistant Blueprint XaaS](#).

Procédure

1 Sélectionnez **Conception > XaaS > Blueprints XaaS**.

2 Cliquez sur l'icône **Nouveau** (+).

3 Dans l'onglet **Workflow**, sélectionnez le workflow qui s'exécute lorsque le Blueprint provisionne la ressource.

Cet onglet n'est pas disponible si vous modifiez un Blueprint.

a Parcourez la bibliothèque de workflows vRealize Orchestrator et sélectionnez un workflow adapté à votre ressource personnalisée.

b Vérifiez les paramètres d'entrée et de sortie pour vous assurer que vous pourrez ultérieurement fournir les valeurs correctes.

c Cliquez sur **Suivant**.

4 Dans l'onglet **Général**, configurez les options et cliquez sur **Suivant**.

a Dans la zone de texte **Nom**, entrez un nom permettant de différencier clairement ce Blueprint.

b Si vous ne souhaitez pas utiliser ce Blueprint en tant que composant dans un Blueprint composite, désélectionnez la case **Rendre disponible comme composant dans le canevas de conception**.

5 Dans l'onglet **Formulaire de Blueprint**, modifiez le formulaire en fonction des besoins et cliquez sur **Suivant**.

6 Dans la page **Ressource provisionnée**, sélectionnez une valeur et cliquez sur **Suivant**.

Option	Description
Aucun provisionnement	Si le workflow ne provisionne pas les ressources, vous pouvez sélectionner cette option ou laisser le champ vide.
<Une ressource personnalisée créée précédemment>	Sélectionnez la ressource personnalisée qui prend en charge ce workflow de provisionnement.

7 Dans l'onglet **Cycle de vie du composant**, définissez comment ce Blueprint se comporte au cours des opérations de réduction/montée en charge et de destruction.

Ces workflows s'exécutent sur un Blueprint composite déployé où ce Blueprint est un composant. La disponibilité des différentes options dépend du Blueprint. Tous les workflows de Blueprint ne prennent pas en charge ou ne nécessitent pas toutes les options.

8 Cliquez sur **Terminer**.

9 Sélectionnez la ligne correspondant à votre Blueprint et cliquez sur **Publier**.

Vous avez créé et publié un Blueprint XaaS.

Suivant

- Pour ajouter ce Blueprint directement au catalogue de services en tant que Blueprint autonome, ajoutez un service et ajoutez le Blueprint à un service. Reportez-vous à [Ajouter un service](#).

- Pour utiliser ce Blueprint en tant que composant dans un Blueprint composite, reportez-vous à [Ajouter un Blueprint XaaS à un Blueprint composite](#).

Options Nouveau et Modifier de l'assistant Blueprint XaaS

Utilisez ces options pour créer un Blueprint XaaS qui exécute un workflow vRealize Orchestrator lorsque le Blueprint est déployé. Le workflow modifie un système cible dans votre environnement.

Pour la procédure de création du Blueprint, reportez-vous à [Ajouter un Blueprint XaaS](#).

Pour utiliser cet assistant, sélectionnez **Concevoir > XaaS > Blueprint XaaS**.

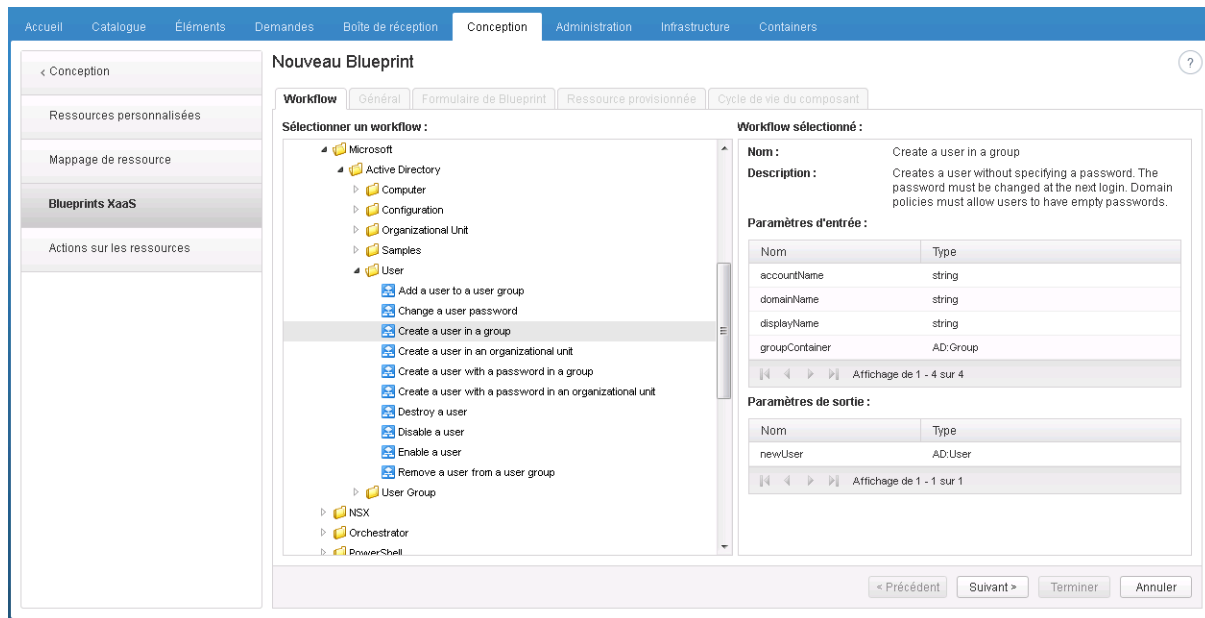
Onglet workflow

Sélectionnez le workflow exécuté lorsque le Blueprint provisionne la ressource.

Cet onglet n'est pas disponible si vous modifiez un Blueprint.

Dans la figure suivante, l'arborescence du workflow est située à gauche et les paramètres à droite.

Figure 3-4. Onglet Blueprint de l'assistant Blueprint XaaS



Vérifiez les paramètres d'entrée et de sortie pour vous assurer que vous ou les utilisateurs de votre catalogue de services peuvent fournir les valeurs correctes dans les circonstances suivantes :

- Si vous personnalisez le formulaire de Blueprint dans cet assistant ou dans le canevas de conception de Blueprint.
- Si vous laissez tous les paramètres d'entrée vides, les utilisateurs du catalogue de services peuvent définir les valeurs.

Onglet Général

Configurez les métadonnées et le comportement du Blueprint.

Tableau 3-57. Options de l'onglet Général

Option	Description
Nom	<p>Nom du Blueprint tel que vous souhaitez qu'il apparaisse dans les emplacements suivants :</p> <ul style="list-style-type: none"> ■ Canevas de conception. Si vous sélectionnez Rendre disponible comme composant dans le canevas de conception, cette valeur est le nom qui apparaît dans la liste des catégories. ■ Services. Si vous utilisez ce Blueprint en tant que Blueprint autonome, cette valeur est le nom qui s'affiche lorsque vous ajoutez des éléments du catalogue au service. ■ Droits d'accès. Si vous autorisez le Blueprint en tant qu'élément individuel, cette valeur est le nom qui s'affiche dans la liste Ajouter des éléments.
Description	Fournissez une description détaillée vous permettant de différencier les éléments similaires.
Masquez la page d'informations de demande de catalogue	Cochez cette case si vous ne souhaitez pas exiger des consommateurs du catalogue de services qu'ils fournissent une description et un motif lorsqu'ils demandent l'élément. La case est cochée par défaut.
Version	Le format pris en charge couvre les version-majeure.version-mineure.micro-version.
Rendre disponible comme composant dans le canevas de conception	<p>Si vous prévoyez d'utiliser le Blueprint en tant que composant dans un Blueprint du canevas de conception, sélectionnez cette option.</p> <p>Lorsqu'il est publié, le Blueprint est disponible dans la catégorie que vous avez sélectionnée lorsque vous avez configuré la ressource personnalisée.</p> <p>Si vous ne sélectionnez pas cette option, le Blueprint n'apparaît pas dans le canevas de conception. Vous pouvez cependant l'ajouter à un service et autoriser les utilisateurs à le déployer en tant que Blueprint autonome.</p>

Onglet Formulaire de Blueprint

Les champs affichés sur cette page de l'assistant sont les paramètres d'entrée du workflow. Vous pouvez apporter les modifications suivantes :

- Ajouter des champs au formulaire.
- Modifier les champs existants en les supprimant ou les réorganisant.
- Fournir des valeurs par défaut comme paramètres d'entrée.

Toutes les modifications affectant le formulaire qui sont présentées :

- L'architecte d'application qui travaille dans le canevas de conception lorsque ce Blueprint XaaS est utilisé en tant que composant de Blueprint.
- L'utilisateur du catalogue de services si ce Blueprint est publié en tant que Blueprint autonome.

Pour plus d'informations sur la configuration des formulaires, reportez-vous à [Conception d'un formulaire de Blueprint XaaS](#).

Ressource provisionnée

La ressource provisionnée relie le Blueprint à une ressource personnalisée XaaS correspondante que vous avez configurée sur la page Ressource personnalisée dans **Concevoir > XaaS > Ressource personnalisée**.

Tableau 3-58. Options de ressource personnalisée

Option	Description
Une ressource personnalisée créée précédemment	<p>Sélectionnez la ressource personnalisée qui définit le type de ressource vRealize Orchestrator requis pour exécuter le Blueprint de provisionnement.</p> <p>Un Blueprint de provisionnement exécute un workflow vRealize Orchestrator pour provisionner des ressources sur le point de terminaison cible à l'aide de l'API de plug-in vRealize Orchestrator pour le point de terminaison. Par exemple, ajoutez des cartes réseau virtuelles à un périphérique réseau dans vSphere.</p> <p>Vous pouvez définir des opérations de post-provisionnement sur ce type de ressources provisionnées. Vous pouvez également rendre le Blueprint évolutif en ajoutant ou supprimant des instances, le cas échéant.</p> <p>Résultats</p> <ul style="list-style-type: none"> ■ Le Blueprint est éligible pour le dimensionnement. ■ Le Blueprint apparaît dans le canevas de conception dans la catégorie spécifiée pour la ressource personnalisée sélectionnée. ■ Le Blueprint est affiché sur l'onglet Éléments lorsque vous déployez un Blueprint qui l'inclut, et vous pouvez exécuter toutes les actions sur l'élément après le déploiement.
Aucun provisionnement	<p>Un Blueprint de non-provisionnement exécute un workflow vRealize Orchestrator pour effectuer une tâche qui ne nécessite pas que l'API apporte des modifications au point de terminaison. Il permet par exemple de créer un rapport puis de l'envoyer par e-mail ou le publier sur un système de communication cible.</p> <p>Résultats</p> <ul style="list-style-type: none"> ■ Le Blueprint n'est pas éligible pour le dimensionnement. Vous pouvez utiliser des Blueprints de non-provisionnement comme workflows de prise en charge dans des Blueprints évolutifs. Par exemple, vous pouvez créer un Blueprint pour mettre à jour un équilibrage de charge à haute disponibilité. ■ Le Blueprint apparaît dans la catégorie XaaS dans le canevas de conception. ■ Le Blueprint n'est pas affiché sur l'onglet Éléments lorsque vous déployez un Blueprint qui l'inclut, et vous ne pouvez pas non plus exécuter d'actions sur l'élément après le déploiement.

Onglet Cycle de vie du composant

L'onglet Cycle de vie du composant est disponible si vous avez sélectionné **Rendre disponible comme composant dans le canevas de conception** dans l'onglet **Général**.

Utilisez ces options pour définir la manière dont le post-déploiement de ce Blueprint sera effectué lors des opérations de réduction de charge et de montée en charge lorsqu'il est utilisé en tant que composant dans un Blueprint composite.

La disponibilité des différentes options dépendent du Blueprint. Tous les workflows de Blueprint ne prennent pas en charge ou ne nécessitent pas toutes les options. Étant donné que votre Blueprint XaaS peut être utilisé dans un Blueprint composite, vous devez configurer les options de mise à jour et de destruction, et également d'allocation et de désallocation, si elles sont disponibles pour le Blueprint afin que celui-ci soit dimensionné correctement.

Tableau 3-59. Options de cycle de vie du composant

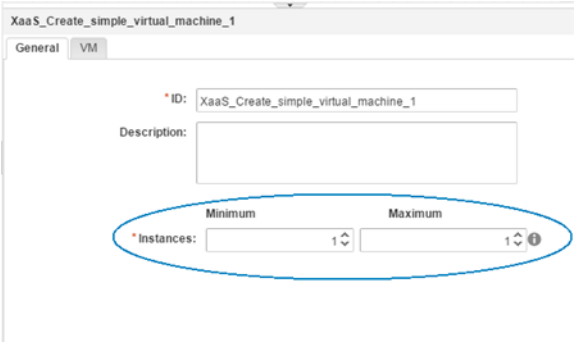
Option	Description
Évolutif	<p>Sélectionnez cette option pour permettre à l'utilisateur du catalogue de services de modifier le nombre d'instances de ce composant de Blueprint après son déploiement lors d'une opération de réduction de charge ou de montée en charge.</p> <p>Cette option est disponible si vous avez sélectionné une ressource personnalisée dans l'onglet Ressource provisionnée. Elle n'est pas disponible si vous avez sélectionné l'option Pas de provisionnement.</p> <p>Si vous rendez ce Blueprint évolutif, l'option Instances est ajoutée sur l'onglet Général dans le canevas de conception. Voir l'exemple ci-dessous. Si vous ne sélectionnez pas l'option Évolutif, l'option Instances n'est pas disponible dans le canevas de conception.</p> 
Workflow de provisionnement	<p>Workflow qui s'exécute lors d'une opération de provisionnement ou de montée en charge. Ce workflow a été sélectionné lorsque vous avez créé ce Blueprint et vous ne pouvez pas modifier la valeur.</p>

Tableau 3-59. Options de cycle de vie du composant (suite)

Option	Description
Workflow d'allocation	<p>Sélectionnez le workflow qui s'exécute avant l'opération de provisionnement ou de montée en charge initiale.</p> <p>Ce type de workflow de cycle de vie est disponible pour les allocations Azure. Si vous créez un workflow d'allocation pour une opération de dimensionnement, il doit inclure les valeurs suivantes :</p> <ul style="list-style-type: none"> ■ Paramètres d'entrée <ul style="list-style-type: none"> ■ Le nom du paramètre est requestData et le type de paramètre est Properties. ■ Le nom du paramètre est subtenant et le type de paramètre est Properties. ■ reservations et le type de paramètre est Arrays/Properties. ■ Paramètre de sortie <ul style="list-style-type: none"> ■ Doit inclure un paramètre du type Properties.
Workflow de mise à jour	<p>Sélectionnez le workflow qui s'exécute lors des opérations de mise à jour, y compris de réduction de charge ou de montée en charge si un composant n'est pas évolutif mais peut être mis à jour.</p> <p>Par exemple, un équilibrage de charge est mis à jour avec la nouvelle configuration créée avec l'opération de réduction de charge ou de montée en charge pour les composants du Blueprint composite.</p> <p>Le workflow de mise à jour peut s'appliquer à un composant qui est lié à un composant dimensionné, mais qui n'est pas lui-même évolutif. Ce workflow de mise à jour peut modifier le composant qui n'est pas évolutif en fonction d'une opération de mise à jour.</p> <p>Si vous créez un workflow de mise à jour pour une opération de dimensionnement, il doit inclure les valeurs suivantes :</p> <ul style="list-style-type: none"> ■ Paramètres d'entrée. <ul style="list-style-type: none"> ■ Doit inclure un paramètre, quel que soit le nom du paramètre, qui correspond au type de paramètre de sortie du workflow de provisionnement. ■ Le nom du paramètre est data et le type de paramètre est Properties.

Tableau 3-59. Options de cycle de vie du composant (suite)

Option	Description
Workflow de destruction	<p>Workflow qui s'exécute lors d'une opération de réduction de charge ou de destruction.</p> <p>Si vous créez un workflow de destruction pour une opération de dimensionnement, il doit inclure la valeur suivante :</p> <ul style="list-style-type: none"> ■ Paramètre d'entrée. <ul style="list-style-type: none"> ■ Doit inclure un paramètre, quel que soit le nom du paramètre, qui correspond au type de paramètre de sortie du workflow de provisionnement. <p>Par exemple, si le workflow Créer un provisionnement de machine virtuelle simple inclut le paramètre de sortie VC:MachineVirtuelle, le workflow de destruction doit inclure un paramètre d'entrée du type VC:MachineVirtuelle.</p>
Workflow de désallocation	<p>Sélectionnez le workflow qui s'exécute après une opération de destruction ou de réduction de charge. Si le processus de désallocation échoue pendant l'opération, le workflow de destruction continue à s'exécuter normalement.</p> <p>La désallocation est le processus final lorsque vous réduisez en charge ou détruisez un Blueprint composite. Ce processus s'exécute après l'opération de destruction, libérant des ressources.</p> <p>Ce type de workflow de cycle de vie est disponible pour les allocations Azure. Si vous créez un workflow de désallocation pour une opération de dimensionnement, il doit inclure la valeur suivante :</p> <ul style="list-style-type: none"> ■ Paramètre d'entrée. <ul style="list-style-type: none"> ■ Le nom du paramètre est <code>data</code> et le type de paramètre est <code>Properties</code>.
Catégorie	<p>Pour spécifier où le Blueprint XaaS apparaît dans le canevas de conception, sélectionnez une valeur dans le menu déroulant Catégorie de canevas de conception.</p> <p>Si vous ne sélectionnez pas de catégorie, le Blueprint est ajouté à la catégorie XaaS lorsqu'il est publié.</p>

Ajouter un Blueprint XaaS à un Blueprint composite

Vous ajoutez un Blueprint XaaS en tant que composant d'un Blueprint composite en suivant une procédure similaire à celle de l'ajout de composants de Blueprint dans le canevas de conception.

Utilisez cette méthode pour ajouter un Blueprint XaaS à un Blueprint composite. Ce Blueprint peut être le seul composant de Blueprint ou faire partie des plusieurs composants formant un Blueprint d'application.

Si vous désirez seulement fournir le Blueprint XaaS à vos utilisateurs, vous pouvez l'ajouter à un service et autoriser les utilisateurs à l'utiliser sans l'ajouter à un Blueprint composite.

Si vous exécutez une opération de réduction de charge ou de montée en charge sur un Blueprint d'application déployé, le Blueprint XaaS se redimensionne en fonction du mode de configuration des options du cycle de vie du Blueprint.

Prérequis

- Connectez-vous à la console vRealize Automation en tant qu'**architecte d'infrastructure**.
- Créez et publiez un Blueprint XaaS. Reportez-vous à [Créer un Blueprint XaaS](#). Lorsque vous créez le Blueprint, vous spécifiez la catégorie dans laquelle le Blueprint est situé dans le canevas de conception.
- Déterminez comment personnaliser les formulaires de Blueprint XaaS dans le Blueprint composite. Reportez-vous à [Conception de formulaires pour les Blueprints XaaS et d'actions associées](#).

Procédure

1 Sélectionnez **Conception > Blueprints**.

2 Sélectionnez le nom du Blueprint auquel vous ajoutez le Blueprint XaaS.

Le canevas de conception s'affiche. Il contient les Blueprints de composant d'application actuels et d'autres composants.

3 Dans la liste Catégories, recherchez le Blueprint.

4 Faites glisser le Blueprint jusqu'au canevas.

5 Configurez les valeurs par défaut dans les onglets Général et Créer.

Ces valeurs par défaut apparaissent dans le formulaire du catalogue de services lorsqu'un utilisateur demande l'élément.

6 Cliquez sur **Terminer**.

7 Sélectionnez le Blueprint et cliquez sur **Publier**.

Le Blueprint XaaS fait désormais partie du Blueprint composite.

Suivant

Ajoutez le Blueprint composite à un service. Reportez-vous à [Gestion du catalogue de services](#).

Créer une action sur la ressource XaaS

Créez une action sur la ressource afin de gérer les éléments provisionnés à l'aide des workflows de vRealize Orchestrator.

Prérequis

- Connectez-vous à la console vRealize Automation en tant qu'**architecte XaaS**.
- Vérifiez que vous disposez d'une ressource personnalisée qui prend en charge l'action. Reportez-vous à [Ajouter une ressource personnalisée XaaS](#).
- Si vous créez des actions à exécuter sur des éléments non provisionnés en tant qu'éléments du catalogue XaaS, vérifiez que vous avez mappé les ressources cibles. Reportez-vous à [Mappage d'autres ressources pour utiliser des actions sur la ressource XaaS](#).

Procédure

1 Créer une action sur les ressources

Une action sur les ressources désigne un workflow XaaS que les utilisateurs du catalogue de services peuvent exécuter sur des éléments de catalogue provisionnés. En tant qu'architecte XaaS, vous pouvez créer des actions sur les ressources pour définir les opérations que les consommateurs peuvent réaliser sur les éléments provisionnés.

2 Publier une action sur la ressource

L'action sur la ressource créée récemment est dans un état de brouillon et vous devez la publier.

3 Attribuer une icône à une action sur les ressources XaaS

Après avoir créé et publié une action sur les ressources, vous pouvez la modifier et attribuer une icône à l'action.

Créer une action sur les ressources

Une action sur les ressources désigne un workflow XaaS que les utilisateurs du catalogue de services peuvent exécuter sur des éléments de catalogue provisionnés. En tant qu'architecte XaaS, vous pouvez créer des actions sur les ressources pour définir les opérations que les consommateurs peuvent réaliser sur les éléments provisionnés.

En créant une action sur les ressources, vous associez un workflow vRealize Orchestrator en tant qu'opération de post-provisionnement. Durant ce processus, vous pouvez modifier les formulaires d'envoi et en lecture seule. Reportez-vous à [Conception d'un formulaire d'action sur la ressource](#).

Prérequis

- Connectez-vous à la console vRealize Automation en tant qu'**architecte XaaS**.
- Créez une ressource personnalisée correspondant au paramètre d'entrée de l'action sur les ressources.

Procédure

1 Sélectionnez **Conception > XaaS > Actions sur les ressources**.

2 Cliquez sur l'icône **Nouveau (+)**.

3 Parcourez la bibliothèque de workflows vRealize Orchestrator et sélectionnez un workflow adapté à votre ressource personnalisée.

Vous pouvez voir le nom et la description du workflow sélectionné, ainsi que les paramètres d'entrée et de sortie tels qu'ils sont définis dans vRealize Orchestrator.

4 Cliquez sur **Suivant**.

5 Sélectionnez la ressource personnalisée que vous avez créée précédemment dans le menu déroulant **Type de ressource**.

6 Sélectionnez le paramètre d'entrée de l'action sur les ressources dans le menu déroulant **Paramètre d'entrée**.

7 Cliquez sur **Suivant**.

8 Entrez un nom et, éventuellement, une description.

Les zones de texte **Nom** et **Description** sont pré-remplies avec le nom et la description des workflows tels qu'ils sont définis dans vRealize Orchestrator.

9 (Facultatif) Si vous ne souhaitez pas inviter les consommateurs à entrer une description et un motif pour demander cette action sur les ressources, cochez la case **Masquez la page d'informations de demande de catalogue**.

10 Entrez une version.

Le format pris en charge couvre les version-majeure.version-mineure.micro-version.

11 (Facultatif) Sélectionnez le type d'action.

Option	Description
Élimination	Le paramètre d'entrée du workflow d'action sur les ressources est éliminé et l'élément est supprimé de l'onglet Éléments . Par exemple, l'action sur les ressources concerne la suppression d'une machine provisionnée.
Provisionnement	L'action sur les ressources concerne le provisionnement. Par exemple, l'action sur les ressources concerne la copie d'un élément du catalogue. Sélectionnez un paramètre de sortie dans le menu déroulant. Vous pouvez sélectionner une ressource personnalisée que vous avez créée précédemment de sorte que lorsque les consommateurs demandent cette action sur les ressources, les éléments provisionnés soient ajoutés à l'onglet Éléments . Si seule l'option Aucun provisionnement est disponible, soit l'action sur les ressources ne concerne pas le provisionnement, soit vous n'avez pas créé une ressource personnalisée adéquate pour le paramètre de sortie, et vous ne pouvez pas continuer.

En fonction du workflow d'action, vous pouvez sélectionner une, deux ou aucune des options.

12 Sélectionnez les conditions dans lesquelles l'action sur les ressources est disponible aux utilisateurs, puis cliquez sur **Suivant**.13 (Facultatif) Modifiez le formulaire de l'action sur les ressources dans l'onglet **Formulaire**.

Le formulaire de l'action sur les ressources mappe la présentation du workflow vRealize Orchestrator. Vous pouvez modifier le formulaire en supprimant, en modifiant et en réorganisant les éléments. Vous pouvez également ajouter un nouveau formulaire et de nouvelles pages de formulaire, ainsi que faire glisser les éléments nécessaires vers le nouveau formulaire et la nouvelle page de formulaire.

Option	Action
Ajouter un formulaire	Cliquez sur l'icône Nouveau formulaire (+) en regard du nom du formulaire, donnez les informations requises, puis cliquez sur Soumettre .
Modifier un formulaire	Cliquez sur l'icône Modifier (✎) en regard du nom du formulaire, effectuez les modifications nécessaires et cliquez sur Soumettre .
Régénérez la présentation du workflow	Cliquez sur l'icône Recréer (↺) en regard du nom du formulaire et cliquez sur OK .

Option	Action
Supprimer un formulaire	Cliquez sur l'icône Supprimer (✖) en regard du nom du formulaire, puis cliquez sur OK dans la boîte de dialogue de confirmation.
Ajouter une page de formulaire	Cliquez sur l'icône Nouvelle page (+) en regard du nom de la page de formulaire, donnez les informations requises, puis cliquez sur Soumettre .
Modifier une page de formulaire	Cliquez sur l'icône Modifier (✎) en regard du nom de la page de formulaire, effectuez les modifications nécessaires et cliquez sur Soumettre .
Supprimer une page de formulaire	Cliquez sur l'icône Supprimer (✖) en regard du nom du formulaire, puis cliquez sur OK dans la boîte de dialogue de confirmation.
Ajouter un élément à la page de formulaire	Faites glisser un élément du panneau Nouveaux champs à gauche vers le panneau de droite. Vous pouvez ensuite fournir les informations requises et cliquer sur Soumettre .
Modifier un élément	Cliquez sur l'icône Modifier (✎) en regard de l'élément à modifier, effectuez les modifications nécessaires et cliquez sur Soumettre .
Supprimer un élément	Cliquez sur l'icône Supprimer (✖) en regard de l'élément à supprimer, puis cliquez sur OK dans la boîte de dialogue de confirmation.

14 Cliquez sur **Terminer**.

Vous avez créé une action sur les ressources et vous pouvez la voir apparaître sur la page Actions sur les ressources.

Suivant

Publiez l'action sur les ressources. Reportez-vous à [Publier une action sur la ressource](#).

Publier une action sur la ressource

L'action sur la ressource créée récemment est dans un état de brouillon et vous devez la publier.

Prérequis

Connectez-vous à la console vRealize Automation en tant qu'**architecte XaaS**.

Procédure

- 1 Sélectionnez **Conception > XaaS > Actions sur les ressources**.
- 2 Sélectionnez la ligne de l'action sur la ressource à publier et cliquez sur **Publier**.

L'état de l'action sur la ressource passe à Publiée.

Suivant

Attribuez une icône à l'action sur la ressource. Reportez-vous à [Attribuer une icône à une action sur les ressources XaaS](#). Les gestionnaires de groupes d'activité et les administrateurs de locataire peuvent ensuite utiliser l'action quand ils créent un droit d'accès.

Attribuer une icône à une action sur les ressources XaaS

Après avoir créé et publié une action sur les ressources, vous pouvez la modifier et attribuer une icône à l'action.

Prérequis

Connectez-vous à la console vRealize Automation en tant qu'**architecte XaaS**.

Procédure

- 1 Sélectionnez **Administration > Gestion de catalogue > Actions**.
- 2 Sélectionnez l'action sur les ressources que vous avez créée.
- 3 Cliquez sur **Configurer**.
- 4 Cliquez sur **Parcourir** et sélectionnez l'icône à ajouter.
- 5 Cliquez sur **Ouvrir**.
- 6 Cliquez sur **Mise à jour**.

Vous avez attribué une icône à l'action sur les ressources. Les gestionnaires de groupes d'activités et les gestionnaires de locataires peuvent utiliser l'action sur les ressources dans une autorisation.

Mappage d'autres ressources pour utiliser des actions sur la ressource XaaS

Mappez les éléments non provisionnés à l'aide de XaaS afin de pouvoir exécuter des actions sur la ressource à opérer sur ces éléments.

Actions et workflows du script de mappage de ressource

Vous pouvez utiliser les mappages de ressources fournis pour les machines virtuelles vSphere, vCloud Director ou vCloud Air. Vous pouvez également créer des actions de script vRealize Orchestrator ou des workflows personnalisés pour mapper d'autres types de ressources du catalogue vRealize Automation à des types d'inventaires vRealize Orchestrator.

Mappages de ressources fournis avec vRealize Automation

vRealize Automation inclut des mappages de ressources pour machines virtuelles vSphere IaaS, pour vCloud Director IaaS et pour des déploiements.

vRealize Automation inclut des actions de script de mappage de ressources vRealize Orchestrator pour chacun des mappages de ressources XaaS fournis. Les actions du script des mappages de ressources fournis sont situés dans le module `com.vmware.vcac.asd.mappings` du serveur vRealize Orchestrator intégré.

Lorsque vous créez une action sur la ressource s'exécutant sur un Blueprint composite déployé utilisant un workflow vRealize Orchestrator avec `vCACAFE:CatalogResource` comme paramètre d'entrée, le mappage du déploiement est appliqué en tant que type de ressource d'entrée. Le mappage du déploiement est uniquement appliqué si le workflow sélectionné inclut `vCACAFE:CatalogResource` en tant que paramètre d'entrée. Par exemple, si vous créez une action pour demander une action sur la ressource au nom d'un utilisateur, le type de ressources sur l'onglet Ressource d'entrée est Déploiement car ce workflow utilise le paramètre `vCACAFE:CatalogResource`.

Les mappages de ressources de machine virtuelle vCD IaaS et VC IaaS sont utilisés par une action pour mapper les machines virtuelles correspondant à la ressource IaaS à la machine virtuelle vRealize Orchestrator, vSphere ou vCloud Director.

Développement de mappages de ressources

En fonction de la version de vRealize Orchestrator, vous pouvez créer un workflow ou une action du script vRealize Orchestrator afin de mapper des ressources entre vRealize Orchestrator et vRealize Automation.

Pour développer le mappage de ressources, utilisez un paramètre d'entrée de type `Properties`. Ce paramètre contient une paire clé-valeur qui définit la ressource provisionnée, et un paramètre de sortie du type d'inventaire d'une instance de vRealize Orchestrator attendu par le plug-in vRealize Orchestrator correspondant. Les propriétés disponibles pour le mappage dépendent du type de ressource. Par exemple, la propriété `EXTERNAL_REFERENCE_ID` est un paramètre de clé courant qui définit des machines virtuelles individuelles. Vous pouvez utiliser cette propriété pour demander une ressource du catalogue. Si vous créez un mappage pour une ressource qui n'utilise aucun `EXTERNAL_REFERENCE_ID`, vous pouvez utiliser l'une des autres propriétés transmises aux machines virtuelles individuelles, telles que le nom, la description, etc.

Pour plus d'informations sur le développement de workflows et de scripts, reportez-vous à *Développement avec VMware vCenter Orchestrator*.

Créer un mappage de ressource

vRealize Automation fournit des mappages de ressources pour les machines vSphere, vCloud Director et vCloud Air. Vous pouvez créer des mappages de ressources supplémentaires pour d'autres types de ressources du catalogue.

Prérequis

- Connectez-vous à la console vRealize Automation en tant qu'**architecte XaaS**.
- Vérifiez que le script ou le workflow de mappage est disponible dans vRealize Orchestrator. Reportez-vous à [Actions et workflows du script de mappage de ressource](#)

Procédure

- 1 Sélectionnez **Conception > XaaS > Mappage de ressource**.
- 2 Cliquez sur l'icône **Nouveau** (+).
- 3 Entrez un nom et, éventuellement, une description.

4 Entrez une version.

Le format pris en charge couvre les version-majeure.version-mineure.micro-version.

5 Dans la zone de texte **Type de ressources du catalogue**, entrez le type de ressources correspondant et appuyez sur Entrée.

Le type de ressources du catalogue s'affiche dans la vue de détails de l'élément provisionné.

6 Dans la zone de texte **Type de la variable dans l'orchestrateur**, entrez le type d'objet vRealize Orchestrator et appuyez sur Entrée.

Il s'agit du paramètre de sortie du workflow du mappage de ressources.

7 (Facultatif) Ajoutez des critères cibles afin de restreindre la disponibilité des actions sur la ressource créées à l'aide de ce mappage de ressources.

Les actions sur la ressource sont également soumises à des restrictions en fonction des approbations et des droits d'accès.

a Sélectionnez **Disponible en fonction des conditions**.

b Sélectionnez le type de condition.

Option	Description
Tous les éléments suivants	Si toutes les clauses que vous avez définies sont respectées, les actions sur la ressource créées à l'aide de ce mappage de ressources sont mises à la disposition de l'utilisateur.
L'un des éléments suivants	Si l'une des clauses que vous avez définies est respectée, les actions sur la ressource créées à l'aide de ce mappage de ressources sont désormais mises à disposition de l'utilisateur.
Pas les éléments suivants	Si la clause que vous avez définie existe, les actions sur la ressource créées à l'aide de ce mappage de ressources ne sont pas disponibles.

c Suivez les invites qui s'affichent afin de créer les clauses et complétez la condition.

8 Sélectionnez l'action de script ou le workflow de votre mappage de ressources dans la bibliothèque vRealize Orchestrator.

9 Cliquez sur **OK**.

Conception de formulaires pour les Blueprints XaaS et d'actions associées

La fonctionnalité XaaS comporte un concepteur de formulaires d'envoi et de détails pour les Blueprints et les actions sur les ressources. Selon la présentation des workflows, le concepteur de formulaire génère de manière dynamique des formulaires et des champs par défaut que vous pouvez utiliser pour modifier les formulaires par défaut.

Vous pouvez créer des formulaires interactifs que les utilisateurs peuvent remplir pour envoyer des éléments du catalogue et des actions sur les ressources. Vous pouvez également créer des formulaires en lecture seule qui définissent les informations que les utilisateurs peuvent afficher sur la vue de détails d'un élément du catalogue ou d'une ressource provisionnée.

La création de ressources personnalisées XaaS entraîne la génération de Blueprints XaaS, d'actions sur les ressources et de formulaires pour les cas d'utilisation courants.

Tableau 3-60. Types d'objets XaaS et formulaires associés

Type d'objet	Formulaire par défaut	Formulaires supplémentaires
Ressource personnalisée	Formulaire de détails de la ressource basé sur les attributs du type d'inventaire du plug-in de vRealize Orchestrator (en lecture seule).	■ Aucun
Blueprint XaaS	Formulaire d'envoi de demande basé sur la présentation du workflow sélectionné.	<ul style="list-style-type: none"> ■ Détails de l'élément du catalogue (lecture seule) ■ Détails de la demande envoyée (lecture seule)
Action sur la ressource	Formulaire d'envoi d'action basé sur la présentation du workflow sélectionné.	■ Détails de l'action envoyée (lecture seule)

Vous pouvez modifier les formulaires par défaut ou concevoir de nouveaux formulaires. Vous pouvez faire glisser les champs à ajouter et les réorganiser sur le formulaire. Vous pouvez définir des contraintes sur les valeurs de certains champs, spécifier des valeurs par défaut ou fournir des instructions à l'attention des utilisateurs finaux qui remplissent le formulaire.

En raison de leurs différentes finalités, les opérations que vous effectuez pour concevoir des formulaires en lecture seule sont limitées par rapport à celles que vous effectuez pour concevoir des formulaires d'envoi.

Champs dans le concepteur de formulaires

Vous pouvez étendre la présentation et la fonctionnalité des workflows en ajoutant de nouveaux champs prédéfinis aux formulaires d'actions sur les ressources et de blueprints XaaS.

Si un paramètre d'entrée est défini dans le workflow vRealize Orchestrator, il apparaît dans le formulaire généré par défaut dans vRealize Automation. Si vous ne souhaitez pas utiliser les champs générés par défaut dans le formulaire, vous pouvez les supprimer et glisser-déposer de nouveaux champs à partir de la palette. Vous pouvez remplacer les champs générés par défaut sans rompre les mappages de workflow si vous utilisez le même identifiant que le champ que vous remplacez.

Vous pouvez également ajouter de nouveaux champs, autres que ceux qui ont été générés en fonction des entrées de workflow vRealize Orchestrator, afin de pouvoir étendre la présentation et la fonctionnalité du workflow dans les cas suivants :

■ Ajouter des contraintes aux champs existants

Par exemple, vous pouvez créer un nouveau menu déroulant et le nommer **dd**. Vous pouvez également créer les options prédéfinies Or, Argent, Bronze et Personnalisé. S'il y a un champ prédéfini, tel que CPU, vous pouvez ajouter les contraintes suivantes à ce champ :

- Si dd est égal à Or, la vitesse du CPU est 2000 MHz
- Si dd est égal à Argent, la vitesse du CPU est 1000 MHz
- Si dd est égal à Bronze, la vitesse du CPU est 500 MHz

- Si dd est égal à Personnalisé, le champ CPU est modifiable, et le consommateur peut spécifier une valeur personnalisée
- Ajouter des définitions de valeurs externes aux champs

Vous pouvez ajouter une définition de valeur externe à un champ afin de pouvoir exécuter des actions de script vRealize Orchestrator et fournir des informations supplémentaires aux consommateurs dans les formulaires que vous concevez. Par exemple, vous pouvez créer un workflow permettant de modifier les paramètres de pare-feu d'une machine virtuelle. Sur la page de demande d'action sur la ressource, vous souhaitez permettre à l'utilisateur de modifier les paramètres de port ouvert, mais vous souhaitez également restreindre les options aux ports qui sont ouverts. Vous pouvez ajouter une définition de valeur externe à un champ à liste double et sélectionner une action de script vRealize Orchestrator qui effectue une requête sur les ports ouverts. Lorsque le formulaire de demande se charge, les actions du script s'exécutent, et les ports ouverts sont présentés comme option à l'utilisateur.

- Ajouter de nouveaux champs qui sont traités dans le workflow vRealize Orchestrator en tant que paramètres globaux

Par exemple, le workflow fournit une intégration à un système tiers et le développeur du workflow a défini des paramètres d'entrée qui doivent être traités dans la généralité des cas, mais a également fourni un moyen pour transmettre les champs personnalisés. Par exemple, dans une zone d'écriture de script, tous les paramètres globaux commençant par **mon_système_tiers** sont traités. Ainsi, si l'architecte XaaS souhaite transmettre des valeurs spécifiques que les consommateurs doivent fournir, l'architecte XaaS peut ajouter un nouveau champ nommé **mon_CPU_tiers**.

Tableau 3-61. Nouveaux champs dans le formulaire d'actions sur les ressources ou de Blueprint XaaS

Champ	Description
Zone de texte	Zone de texte à ligne unique
Zone de texte	Zone de texte multi-ligne
Lien	Champ dans lequel les consommateurs entrent une URL
E-mail	Champ dans lequel les consommateurs entrent une adresse e-mail
Champ de mot de passe	Champ dans lequel les consommateurs entrent un mot de passe
Champ de nombres entiers	Zone de texte dans laquelle les consommateurs entrent un nombre entier Vous pouvez faire de ce champ un curseur avec une valeur minimale et maximale, ainsi qu'un incrément.
Champ de valeurs décimales	Zone de texte dans laquelle les consommateurs entrent une valeur décimale Vous pouvez faire de ce champ un curseur avec une valeur minimale et maximale, ainsi qu'un incrément.
Date et heure	Zones de texte dans lesquelles les consommateurs spécifient une date (en sélectionnant une date dans un menu de calendrier) et peuvent également sélectionner l'heure (à l'aide des flèches vers le haut et vers le bas)

Tableau 3-61. Nouveaux champs dans le formulaire d'actions sur les ressources ou de Blueprint XaaS (suite)

Champ	Description
Liste double	Générateur de liste dans lequel les consommateurs déplacent un ensemble prédéfini de valeurs entre deux listes, la première liste contenant toutes les options non sélectionnées et la seconde les choix de l'utilisateur.
Case à cocher	Case à cocher
Oui/Non	Menu déroulant permettant de sélectionner Oui ou Non
Liste déroulante	Menu déroulant
Liste	Liste
Liste de cases à cocher	Liste de cases à cocher
Groupe de boutons radio	Groupe de boutons radio
Recherche	Zone de texte de recherche renseignant automatiquement la requête et où les consommateurs sélectionnent un objet
Arborescence	Arborescence que les consommateurs utilisent pour rechercher et sélectionner les objets disponibles
Mapper	Table de mappage que les consommateurs utilisent pour définir des paires clé-valeur pour les propriétés

Vous pouvez également utiliser le champ de formulaire **En-tête de section** pour diviser les pages du formulaire en sections avec des en-têtes distincts et le champ de formulaire **Texte** pour ajouter des textes d'information en lecture seule.

Contraintes et valeurs du concepteur de formulaire

Lorsque vous modifiez un élément du Blueprint ou du formulaire d'action sur les ressources, vous pouvez appliquer plusieurs contraintes et valeurs à l'élément.

Contraintes

Les contraintes que vous pouvez appliquer à un élément varient selon le type d'élément que vous modifiez ou que vous ajoutez au formulaire. Il se peut que certaines valeurs de contrainte soient configurées dans le workflow de vRealize Orchestrator. Ces valeurs n'apparaissent pas sur l'onglet Contraintes car elles dépendent souvent de conditions qui sont évaluées alors que le workflow s'exécute. Les valeurs de contrainte que vous configurez pour le formulaire de Blueprint remplacent toute contrainte spécifiée dans le workflow vRealize Orchestrator.

Pour chaque contrainte que vous appliquez à un élément, vous pouvez sélectionner l'une des options suivantes pour la définir :

Non définie	Obtient la propriété de la présentation du workflow vRealize Orchestrator.
Constante	Définit l'élément que vous modifiez comme étant obligatoire ou facultatif.

Champ	Lie l'élément à un autre élément du formulaire. Par exemple, vous pouvez définir l'élément comme étant obligatoire uniquement lorsqu'un autre élément, comme une case à cocher, est sélectionné.
Conditionnelle	Applique une condition. Utilisez les conditions pour créer plusieurs clauses et expressions, puis appliquez-les à l'état ou aux contraintes de l'élément.
Externe	Sélectionnez une action de script vRealize Orchestrator pour définir la valeur.

Tableau 3-62. Contraintes du concepteur de formulaire

Contrainte	Description
Obligatoire	Indique si l'élément est obligatoire.
Lecture seule	Indique si le champ est en lecture seule.
Valeur	Définit une valeur pour l'élément.
Visible	<p>Indique si le consommateur peut voir l'élément.</p> <p>Si vous appliquez une contrainte de visibilité à un groupe d'affichage dans le workflow vRealize Orchestrator, la contrainte est ignorée dans le formulaire Détails de la demande envoyée XaaS et les champs que vous voulez masquer s'affichent dans le formulaire.</p> <p>Pour masquer les champs que vous ne souhaitez afficher dans le formulaire Détails de demande envoyée et qui ne sont pas requis pour l'utilisateur demandeur, supprimez les champs du formulaire Détails de demande envoyée de l'onglet Formulaire de Blueprints dans le concepteur de Blueprint XaaS. Pour localiser cet onglet, reportez-vous à la section Ajouter un nouveau formulaire de Blueprint XaaS.</p>
Longueur minimale	Définit le nombre minimal de caractères de l'élément d'entrée de chaîne.
Longueur maximale	Définit le nombre maximal de caractères de l'élément d'entrée de chaîne.
Valeur minimale	Définit la valeur minimale de l'élément d'entrée de nombre.
Valeur maximale	Définit la valeur maximale de l'élément d'entrée de nombre.
Incrément	Définit un incrément pour un élément comme un champ Décimal ou Entier . Par exemple, si vous souhaitez qu'un champ Entier soit généré en tant que Curseur , vous pouvez utiliser la valeur du pas.
Nombre minimal	<p>Définit un nombre minimal d'éléments pouvant être sélectionnés.</p> <p>Par exemple, lorsque vous ajoutez ou modifiez une Liste de cases à cocher, vous pouvez définir le nombre minimum de cases à cocher que le consommateur doit sélectionner pour continuer.</p>
Nombre maximal	<p>Définit un nombre maximal d'éléments pouvant être sélectionnés.</p> <p>Par exemple, lorsque vous ajoutez ou modifiez une Liste de cases à cocher, vous pouvez définir le nombre maximum de cases à cocher que le consommateur doit sélectionner pour continuer.</p>

Valeurs

Vous pouvez appliquer des valeurs à certains éléments et définir ce que les consommateurs voient pour certains champs. Les options disponibles varient en fonction du type d'élément que vous modifiez ou que vous ajoutez au formulaire.

Tableau 3-63. Valeurs du concepteur de formulaire

Valeur	Description
Non définie	Obtient la valeur de l'élément que vous modifiez dans la présentation du workflow vRealize Orchestrator.
Valeurs prédéfinies	Sélectionnez les valeurs dans une liste d'objets associés dans l'inventaire vRealize Orchestrator.
Valeur	Définit des valeurs statiques personnalisées avec des étiquettes.
Valeurs externes	Sélectionnez une action de script vRealize Orchestrator qui définit votre valeur avec des informations qui ne sont pas directement exposées par le workflow.

Définitions de valeurs externes dans le concepteur de formulaires

Lorsque vous éditez certains éléments dans le concepteur de formulaires, vous pouvez attribuer des définitions de valeurs externes qui utilisent des actions de script vRealize Orchestrator personnalisées pour fournir les informations qui ne sont pas exposées directement par le workflow.

Par exemple, vous pouvez publier une action sur la ressource pour installer des logiciels sur une machine provisionnée. Au lieu de fournir au consommateur une liste statique de tous les logiciels disponibles pour le téléchargement, vous pouvez remplir dynamiquement cette liste avec les logiciels qui sont appropriés pour le système d'exploitation de la machine, les logiciels que l'utilisateur n'a pas installé auparavant sur la machine ou les logiciels qui sont périmés sur la machine et qui doivent être mis à jour.

Pour fournir le contenu dynamique à votre consommateur, vous créez une action de script vRealize Orchestrator qui récupère les informations que vous souhaitez afficher pour vos consommateurs. Vous attribuez votre action de script à un champ dans le concepteur de formulaires en tant que définition de valeur externe. Lorsque le formulaire de ressource ou de blueprint de service est présenté à vos consommateurs, l'action de script récupère vos informations personnalisées et les affiche pour votre consommateur.

Vous pouvez utiliser des définitions de valeurs externes pour fournir des valeurs par défaut ou en lecture seule, pour créer des expressions booléennes, pour définir des contraintes ou pour permettre aux consommateurs de sélectionner des éléments dans des listes, de cocher des cases, etc.

Utilisation du concepteur de formulaire

Lorsque vous créez des Blueprints XaaS, des actions sur les ressources personnalisées et des ressources personnalisées, vous pouvez modifier les formulaires des Blueprints, des actions et des ressources à l'aide du concepteur de formulaire. Vous pouvez modifier la représentation et définir ce que les consommateurs de l'élément ou de l'action voient lorsqu'ils demandent l'élément du catalogue ou qu'ils exécutent l'opération de post-provisionnement.

Par défaut, les formulaires de Blueprints XaaS, d'actions sur les ressources et de ressources personnalisées sont générés en fonction de la présentation du workflow de vRealize Orchestrator.

Les différentes étapes de la présentation vRealize Orchestrator sont représentées sous forme de pages et les groupes de présentation vRealize Orchestrator sont représentés sous forme de sections distinctes. Les types d'entrées du workflow sélectionné sont affichées sous la forme de différents champs dans le formulaire. Par exemple, le type vRealize Orchestrator type `string` est représenté par une zone de texte. Un type complexe comme `VC:VirtualMachine` est représenté par une zone de recherche ou une arborescence, afin que le consommateurs puisse taper une valeur alphanumérique pour rechercher une machine virtuelle ou accéder à une machine virtuelle pour la sélectionner.

Create cluster - Modifier le Blueprint

Vous pouvez modifier la représentation d'un objet dans le concepteur de formulaire. Par exemple, vous pouvez modifier la représentation de VC:VirtualMachine par défaut et remplacer la zone de recherche par une arborescence. Vous pouvez également ajouter de nouveaux champs comme des cases à cocher, des menus déroulants, etc. et appliquer différentes contraintes. Si les champs que vous ajoutez ne sont pas valides ou ne sont pas mappés correctement aux entrées du workflow de vRealize Orchestrator, lorsque le consommateur exécute le workflow, vRealize Orchestrator ignore les champs non valides ou non mappés.

Conception d'un formulaire de ressource personnalisée

Tous les champs du formulaire des détails de la ressource sont affichés en lecture seule pour les consommateurs sur la page des détails des éléments lorsqu'ils provisionnent votre ressource personnalisée. Vous pouvez effectuer des opérations de modification de base dans le formulaire, telles que supprimer, modifier ou réorganiser les champs, ou vous pouvez ajouter de nouveaux champs définis en externe qui utilisent les actions de script vRealize Orchestrator pour fournir des informations en lecture seule supplémentaires aux consommateurs.

- [Modifier un élément de ressource personnalisée](#)

Vous pouvez éditer certaines des caractéristiques d'un élément sur la page Formulaire de détails de ressource personnalisée. Chaque champ par défaut sur la page représente une propriété de la ressource personnalisée. Vous ne pouvez pas modifier le type d'une propriété ni les valeurs par défaut, mais vous pouvez modifier le nom, la taille et la description.

- [Ajouter une nouvelle page de formulaire de ressources personnalisées](#)

Vous pouvez ajouter une nouvelle page pour réorganiser le formulaire en plusieurs onglets.

- [Insérer un en-tête de section dans un formulaire de ressources personnalisées](#)

Vous pouvez insérer un en-tête de section pour diviser le formulaire en sections.

- [Insérer un élément de texte dans un formulaire de ressources personnalisées](#)

Vous pouvez insérer une zone de texte afin d'ajouter des observations descriptives au formulaire.

- [Insérer un champ défini en externe dans un formulaire de ressource personnalisée](#)

Vous pouvez insérer un nouveau champ et lui attribuer une définition de valeur externe pour fournir dynamiquement des informations en lecture seule, que les consommateurs peuvent voir sur la page des détails de l'élément lorsqu'ils provisionnent une ressource personnalisée.

Modifier un élément de ressource personnalisée

Vous pouvez éditer certaines des caractéristiques d'un élément sur la page Formulaire de détails de ressource personnalisée. Chaque champ par défaut sur la page représente une propriété de la ressource personnalisée. Vous ne pouvez pas modifier le type d'une propriété ni les valeurs par défaut, mais vous pouvez modifier le nom, la taille et la description.

Prérequis

- Connectez-vous à la console vRealize Automation en tant **qu'administrateur de locataire** ou **architecte XaaS**.
- [Ajouter une ressource personnalisée XaaS](#).

Procédure

- 1 Sélectionnez **Conception > XaaS > Ressources personnalisées**.
- 2 Cliquez sur la ressource personnalisée à modifier.
- 3 Cliquez sur l'onglet **Formulaire de détails**.
- 4 Placez votre curseur sur l'élément que vous souhaitez modifier et cliquez sur l'icône **Modifier**.
- 5 Pour modifier le libellé, entrez le nouveau nom du champ dans la zone de texte **Étiquette**.
- 6 Modifiez la description dans la zone de texte **Description**.
- 7 Sélectionnez une option dans le menu déroulant **Taille** pour modifier la taille de l'élément.
- 8 Sélectionnez une option dans le menu déroulant **Taille d'étiquette** pour modifier la taille de l'étiquette.
- 9 Cliquez sur **Envoyer**.
- 10 Cliquez sur **Terminer**.

Ajouter une nouvelle page de formulaire de ressources personnalisées

Vous pouvez ajouter une nouvelle page pour réorganiser le formulaire en plusieurs onglets.

Prérequis

- Connectez-vous à la console vRealize Automation en tant **qu'administrateur de locataire** ou **architecte XaaS**.
- [Ajouter une ressource personnalisée XaaS](#).

Procédure

- 1 Sélectionnez **Conception > XaaS > Ressources personnalisées**.
- 2 Cliquez sur la ressource personnalisée à modifier.
- 3 Cliquez sur l'onglet **Formulaire de détails**.
- 4 Cliquez sur l'icône **Nouvelle page** (+) en regard du nom de la **page de formulaire**.
- 5 Sélectionnez le type d'écran non utilisé et cliquez sur **Envoyer**.

Si vous possédez déjà une vue Détails des ressources ou Liste des ressources, vous ne pouvez pas créer deux écrans du même type.

- 6 Cliquez sur **Envoyer**.
- 7 Configurez le formulaire.
- 8 Cliquez sur **Terminer**.

Vous pouvez supprimer certains éléments de la page de formulaire originale et les insérer dans la nouvelle page de formulaire, ou vous pouvez ajouter de nouveaux champs qui utilisent des définitions de valeurs externes pour fournir des informations aux consommateurs qui ne sont pas directement affichées par le workflow vRealize Orchestrator.

Insérer un en-tête de section dans un formulaire de ressources personnalisées

Vous pouvez insérer un en-tête de section pour diviser le formulaire en sections.

Prérequis

- Connectez-vous à la console vRealize Automation en tant **qu'administrateur de locataire** ou **architecte XaaS**.
- [Ajouter une ressource personnalisée XaaS](#).

Procédure

- 1 Sélectionnez **Conception > XaaS > Ressources personnalisées**.
- 2 Cliquez sur la ressource personnalisée à modifier.
- 3 Cliquez sur l'onglet **Formulaire de détails**.
- 4 Faites glisser l'élément **En-tête de section** du panneau Formulaire vers le panneau de la page Formulaire.
- 5 Tapez un nom pour la section.
- 6 Cliquez en dehors de l'élément pour enregistrer les modifications.
- 7 Cliquez sur **Terminer**.

Insérer un élément de texte dans un formulaire de ressources personnalisées

Vous pouvez insérer une zone de texte afin d'ajouter des observations descriptives au formulaire.

Prérequis

- Connectez-vous à la console vRealize Automation en tant **qu'administrateur de locataire** ou **architecte XaaS**.
- [Ajouter une ressource personnalisée XaaS](#).

Procédure

- 1 Sélectionnez **Conception > XaaS > Ressources personnalisées**.
- 2 Cliquez sur la ressource personnalisée à modifier.
- 3 Cliquez sur l'onglet **Formulaire de détails**.
- 4 Faites glisser l'élément **Texte** du panneau Formulaire vers le panneau de la page Formulaire.
- 5 Entrez le texte à ajouter.
- 6 Cliquez en dehors de l'élément pour enregistrer les modifications.

7 Cliquez sur **Terminer**.

Insérer un champ défini en externe dans un formulaire de ressource personnalisée

Vous pouvez insérer un nouveau champ et lui attribuer une définition de valeur externe pour fournir dynamiquement des informations en lecture seule, que les consommateurs peuvent voir sur la page des détails de l'élément lorsqu'ils provisionnent une ressource personnalisée.

Prérequis

- Connectez-vous à la console vRealize Automation en tant **qu'administrateur de locataire** ou **architecte XaaS**.
- [Ajouter une ressource personnalisée XaaS](#).
- Développez ou importez une action de script vRealize Orchestrator pour récupérer les informations que vous souhaitez fournir aux consommateurs.

Procédure

- 1 Sélectionnez **Conception > XaaS > Ressources personnalisées**.
- 2 Cliquez sur la ressource personnalisée à modifier.
- 3 Cliquez sur l'onglet **Formulaire de détails**.
- 4 Faites glisser un élément du panneau Nouveaux champs et déposez-le dans le panneau de la page Formulaire.
- 5 Entrez un identifiant pour l'élément dans la zone de texte **ID**.
- 6 Entrez une étiquette dans la zone de texte **Étiquette**.
Les étiquettes sont visibles aux consommateurs sur les formulaires.
- 7 (Facultatif) Sélectionnez le type de champ dans le menu déroulant **Type**.
- 8 Entrez le type de résultat de votre action de script vRealize Orchestrator dans la zone de recherche **Type d'entité** et appuyez sur la touche Entrée.
Par exemple, si vous souhaitez utiliser une action de script pour afficher l'utilisateur actuel, et que le script renvoie le type de résultat vRealize Orchestrator LdapUser, entrez **LdapUser** dans la zone de recherche **Type d'entité** et appuyez sur la touche Entrée.
- 9 Cliquez sur **Ajouter une valeur externe**.
- 10 Sélectionnez votre action de script vRealize Orchestrator personnalisée
- 11 Cliquez sur **Envoyer**.
- 12 Cliquez de nouveau sur **Envoyer**.
- 13 Cliquez sur **Terminer**.

Lorsque le formulaire est présenté à vos consommateurs, l'action de script récupère vos informations personnalisées et les affiche pour votre consommateur.

Conception d'un formulaire de Blueprint XaaS

Lorsque vous créez un Blueprint XaaS, vous pouvez modifier son formulaire en ajoutant de nouveaux champs, en modifiant les champs existants, en les supprimant ou en les réorganisant. Vous pouvez également créer de nouveaux formulaires et pages de formulaire, et y glisser-déposer de nouveaux champs.

- [Ajouter un nouveau formulaire de Blueprint XaaS](#)

Lorsque vous modifiez le formulaire généré par défaut d'un workflow que vous souhaitez publier comme Blueprint XaaS, vous pouvez ajouter un nouveau formulaire de Blueprint XaaS.

- [Modifier un élément du Blueprint XaaS](#)

Vous pouvez modifier certaines caractéristiques d'un élément sur la page Formulaire de Blueprint d'un Blueprint XaaS. Vous pouvez modifier le type d'un élément, ses valeurs par défaut, et appliquer différentes contraintes et valeurs.

- [Ajouter un nouvel élément](#)

Lorsque vous modifiez le formulaire généré par défaut d'un Blueprint XaaS, vous pouvez ajouter un nouvel élément prédéfini au formulaire. Par exemple, pour ne pas utiliser un champ généré par défaut, supprimez ce champ et remplacez-le par un nouveau.

- [Insérer un en-tête de section dans un formulaire de Blueprint XaaS](#)

Vous pouvez insérer un en-tête de section pour diviser le formulaire en sections.

- [Ajouter un élément de texte à un formulaire de Blueprint XaaS](#)

Vous pouvez insérer une zone de texte afin d'ajouter des observations descriptives au formulaire.

Ajouter un nouveau formulaire de Blueprint XaaS

Lorsque vous modifiez le formulaire généré par défaut d'un workflow que vous souhaitez publier comme Blueprint XaaS, vous pouvez ajouter un nouveau formulaire de Blueprint XaaS.

En ajoutant un nouveau formulaire de Blueprint XaaS, vous définissez l'apparence des détails de l'élément du catalogue et les pages des détails de la demande envoyée. Si vous n'ajoutez pas un formulaire de détails de l'élément du catalogue et de détails de la demande envoyée, le consommateur voit ce qui est défini dans le formulaire de demande.

Prérequis

- Connectez-vous à la console vRealize Automation en tant **qu'administrateur de locataire ou architecte XaaS**.
- [Ajouter un Blueprint XaaS](#).

Procédure

- 1 Sélectionnez **Conception > XaaS > Blueprints XaaS**.
- 2 Cliquez sur le XaaSBlueprint à modifier.
- 3 Cliquez sur l'onglet **Formulaire de Blueprint**.
- 4 Cliquez sur l'icône **Nouveau formulaire (+)**.

- 5 Entrez un nom et, éventuellement, une description.
- 6 Sélectionnez le type d'écran dans le menu **Type d'écran**.

Option	Description
Détails de l'élément du catalogue	Une page de détails de l'élément du catalogue que les consommateurs voient lorsqu'ils cliquent sur un élément du catalogue.
Formulaire de demande	Le formulaire de Blueprint XaaS par défaut. Les consommateurs voient le formulaire de demande lorsqu'ils demandent l'élément du catalogue.
Détails de la demande envoyée	Une page de détails de la demande que les consommateurs voient après avoir demandé l'élément, s'ils souhaitent afficher les détails de la demande dans l'onglet Demande .

- 7 Cliquez sur **Envoyer**.

Suivant

Ajoutez les champs de votre choix en les glissant depuis le panneau Nouveaux champs vers le panneau de la page Formulaire.

Modifier un élément du Blueprint XaaS

Vous pouvez modifier certaines caractéristiques d'un élément sur la page Formulaire de Blueprint d'un Blueprint XaaS. Vous pouvez modifier le type d'un élément, ses valeurs par défaut, et appliquer différentes contraintes et valeurs.

Prérequis

- Connectez-vous à la console vRealize Automation en tant **qu'administrateur de locataire** ou **architecte XaaS**.
- [Ajouter un Blueprint XaaS](#).

Procédure

- 1 Sélectionnez **Conception > XaaS > Blueprints XaaS**.
- 2 Cliquez sur le XaaSBlueprint à modifier.
- 3 Cliquez sur l'onglet **Formulaire de Blueprint**.
- 4 Cliquez sur l'élément à modifier.
- 5 Cliquez sur l'icône **Modifier** (✎).
- 6 Entrez un nouveau nom pour le champ dans la zone de texte **Étiquette** pour modifier l'étiquette que les consommateurs voient.
- 7 Modifiez la description dans la zone de texte **Description**.
- 8 Sélectionnez une option dans le menu déroulant **Type** pour modifier le type d'affichage de l'élément. Les options varient en fonction du type d'élément que vous modifiez.
- 9 Sélectionnez une option dans le menu déroulant **Taille** pour modifier la taille de l'élément.

10 Sélectionnez une option dans le menu déroulant **Taille d'étiquette** pour modifier la taille de l'étiquette.

11 Modifiez la valeur par défaut de l'élément.

Option	Description
Non définie	Obtient la valeur de l'élément que vous modifiez dans la présentation du workflow vRealize Orchestrator.
Constante	Définit la valeur par défaut de l'élément que vous modifiez dans une valeur constante que vous spécifiez.
Champ	Lie la valeur par défaut de l'élément à un paramètre d'un autre élément de la représentation.
Conditionnelle	Applique une condition. En utilisant des conditions, vous pouvez créer plusieurs clauses et expressions, puis les appliquer à un élément.
Externe	Sélectionnez une action de script vRealize Orchestrator pour définir la valeur.

12 Appliquer des contraintes à l'élément dans l'onglet **Contraintes**.

Option	Description
Non définie	Obtient la valeur de l'élément que vous modifiez dans la présentation du workflow vRealize Orchestrator.
Constante	Définit la valeur par défaut de l'élément que vous modifiez dans une valeur constante que vous spécifiez.
Champ	Lie la valeur par défaut de l'élément à un paramètre d'un autre élément de la représentation.
Conditionnelle	Applique une condition. En utilisant des conditions, vous pouvez créer plusieurs clauses et expressions, puis les appliquer à un élément.
Externe	Sélectionnez une action de script vRealize Orchestrator pour définir la valeur.

13 Ajouter une ou plusieurs valeurs à l'élément dans l'onglet **Valeurs**.

Les options disponibles varient en fonction du type d'élément que vous modifiez.

Option	Description
Non définie	Obtient la valeur de l'élément que vous modifiez dans la présentation du workflow vRealize Orchestrator.
Valeurs prédéfinies	<p>Sélectionnez les valeurs dans une liste d'objets associés dans l'inventaire vRealize Orchestrator.</p> <ul style="list-style-type: none"> a Entrez une valeur dans la zone de recherche Valeurs prédéfinies pour rechercher l'inventaire vRealize Orchestrator. b Sélectionnez une valeur dans les résultats de la recherche et appuyez sur Entrée.

Option	Description
Valeur	<p>Définissez des valeurs personnalisées avec des étiquettes.</p> <ol style="list-style-type: none"> Entrez une valeur dans la zone de texte Valeur. Entrez une étiquette pour la valeur dans la zone de texte Étiquette. Cliquez sur l'icône Ajouter (+).
Valeurs externes	<p>Sélectionnez une action de script vRealize Orchestrator pour définir votre valeur avec des informations qui ne sont pas directement exposées par le workflow.</p> <ul style="list-style-type: none"> Sélectionnez Ajouter une valeur externe. Sélectionnez votre action de script vRealize Orchestrator. Cliquez sur Soumettre.

14 Cliquez sur **Envoyer**.

15 Cliquez sur **Terminer**.

Ajouter un nouvel élément

Lorsque vous modifiez le formulaire généré par défaut d'un Blueprint XaaS, vous pouvez ajouter un nouvel élément prédéfini au formulaire. Par exemple, pour ne pas utiliser un champ généré par défaut, supprimez ce champ et remplacez-le par un nouveau.

Prérequis

- Connectez-vous à la console vRealize Automation en tant **qu'administrateur de locataire** ou **architecte XaaS**.
- [Ajouter un Blueprint XaaS](#).

Procédure

- 1 Sélectionnez **Conception > XaaS > Blueprints XaaS**.
- 2 Cliquez sur le XaaSBlueprint à modifier.
- 3 Cliquez sur l'onglet **Formulaire de Blueprint**.
- 4 Faites glisser un élément du panneau Nouveaux champs et déposez-le dans le panneau de la page Formulaire.
- 5 Entrez l'ID d'un paramètre d'entrée de workflow dans la zone de texte **ID**.
- 6 Entrez une étiquette dans la zone de texte **Étiquette**.
Les étiquettes sont visibles aux consommateurs sur les formulaires.
- 7 (Facultatif) Sélectionnez le type de champ dans le menu déroulant **Type**.

- 8 Entrez un objet vRealize Orchestrator dans la zone de texte **Type d'entité** et appuyez sur Entrée.

Cette étape n'est pas obligatoire pour tous les types de champs.

Option	Description
Type de résultat	Si vous utilisez une action de script pour définir une valeur externe pour le champ, entrez le type de résultat de votre action de script vRealize Orchestrator.
Paramètre d'entrée	Si vous utilisez le champ pour accepter la saisie du consommateur et transmettre les paramètres à vRealize Orchestrator, entrez le type de paramètre d'entrée accepté par le workflow vRealize Orchestrator.
Paramètre de sortie	Si vous utilisez le champ pour afficher des informations pour les consommateurs, entrez le type de paramètre de sortie du workflow vRealize Orchestrator.

- 9 (Facultatif) Cochez la case **Valeurs multiples** pour permettre aux consommateurs de sélectionner plusieurs objets.

Cette option n'est pas disponible pour tous les types de champs.

- 10 Cliquez sur **Envoyer**.

- 11 Cliquez sur **Mise à jour**.

Suivant

Vous pouvez modifier l'élément afin de changer les paramètres par défaut et appliquer diverses contraintes ou valeurs.

Insérer un en-tête de section dans un formulaire de Blueprint XaaS

Vous pouvez insérer un en-tête de section pour diviser le formulaire en sections.

Prérequis

- Connectez-vous à la console vRealize Automation en tant **qu'administrateur de locataire** ou **architecte XaaS**.
- [Ajouter un Blueprint XaaS](#).

Procédure

- 1 Sélectionnez **Conception > XaaS > Blueprints XaaS**.
- 2 Cliquez sur le XaaSBlueprint à modifier.
- 3 Cliquez sur l'onglet **Formulaire de Blueprint**.
- 4 Faites glisser l'élément **En-tête de section** du panneau Formulaire vers le panneau de la page Formulaire.
- 5 Tapez un nom pour la section.
- 6 Cliquez en dehors de l'élément pour enregistrer les modifications.
- 7 Cliquez sur **Mise à jour**.

Ajouter un élément de texte à un formulaire de Blueprint XaaS

Vous pouvez insérer une zone de texte afin d'ajouter des observations descriptives au formulaire.

Prérequis

- Connectez-vous à la console vRealize Automation en tant **qu'administrateur de locataire** ou **architecte XaaS**.
- [Ajouter un Blueprint XaaS](#).

Procédure

- 1 Sélectionnez **Conception > XaaS > Blueprints XaaS**.
- 2 Cliquez sur le XaaSBlueprint à modifier.
- 3 Cliquez sur l'onglet **Formulaire de Blueprint**.
- 4 Faites glisser l'élément **Texte** du panneau Nouveaux champs vers le panneau de la page Formulaire.
- 5 Entrez le texte à ajouter.
- 6 Cliquez en dehors de l'élément pour enregistrer les modifications.
- 7 Cliquez sur **Mise à jour**.

Conception d'un formulaire d'action sur la ressource

Lorsque vous créez une action sur la ressource, vous pouvez modifier le formulaire de l'action en ajoutant de nouveaux champs au formulaire, en modifiant les champs existants, en supprimant ou en réorganisant les champs. Vous pouvez également créer de nouveaux formulaires et pages de formulaire, et y glisser-déposer de nouveaux champs.

Ajouter un nouveau formulaire d'action sur les ressources

Lorsque vous modifiez le formulaire généré par défaut d'un workflow que vous souhaitez publier comme action sur les ressources, vous pouvez ajouter un nouveau formulaire d'action sur les ressources.

En ajoutant un nouveau formulaire d'action sur les ressources, vous définissez l'apparence de la page de détails des actions envoyées. Si vous n'ajoutez pas un formulaire de détails des actions envoyées, le consommateur voit ce qui est défini dans le formulaire d'action.

Prérequis

- Connectez-vous à la console vRealize Automation en tant **qu'administrateur de locataire** ou **architecte XaaS**.
- [Créer une action sur les ressources](#).

Procédure

- 1 Sélectionnez **Conception > XaaS > Actions sur les ressources**.
- 2 Cliquez sur l'action sur la ressource à modifier.
- 3 Cliquez sur l'onglet **Formulaire**.

- 4 Cliquez sur l'icône **Nouveau formulaire** (+).
- 5 Entrez un nom et, éventuellement, une description.
- 6 Sélectionnez le type d'écran dans le menu **Type d'écran**.

Option	Description
Formulaire d'action	Le formulaire d'action sur les ressources par défaut que les consommateurs voient lorsqu'ils décident d'exécuter l'action de post-provisionnement
Détails de l'action envoyée	Une page de détails de la demande que les consommateurs voient lorsqu'ils demandent l'action et décident de voir les détails de la demande dans l'onglet Demande .

- 7 Cliquez sur **Envoyer**.

Suivant

Ajoutez les champs de votre choix en les glissant depuis le panneau Nouveaux champs vers le panneau de la page Formulaire.

Ajouter un nouvel élément à un formulaire d'action sur la ressource

Lorsque vous modifiez le formulaire généré par défaut d'une action sur la ressource, vous pouvez ajouter un nouvel élément prédéfini au formulaire. Par exemple, pour ne pas utiliser un champ généré par défaut, supprimez ce champ et remplacez-le par un nouveau.

Prérequis

- Connectez-vous à la console vRealize Automation en tant **qu'administrateur de locataire ou architecte XaaS**.
- [Créer une action sur les ressources](#).

Procédure

- 1 Sélectionnez **Conception > XaaS > Actions sur les ressources**.
- 2 Cliquez sur l'action sur la ressource à modifier.
- 3 Cliquez sur l'onglet **Formulaire**.
- 4 Faites glisser un élément du panneau Nouveaux champs et déposez-le dans le panneau de la page Formulaire.
- 5 Entrez l'ID d'un paramètre d'entrée de workflow dans la zone de texte **ID**.
- 6 Entrez une étiquette dans la zone de texte **Étiquette**.
Les étiquettes sont visibles aux consommateurs sur les formulaires.
- 7 (Facultatif) Sélectionnez le type de champ dans le menu déroulant **Type**.

- 8 Entrez un objet vRealize Orchestrator dans la zone de texte **Type d'entité** et appuyez sur Entrée.

Cette étape n'est pas obligatoire pour tous les types de champs.

Option	Description
Type de résultat	Si vous utilisez une action de script pour définir une valeur externe pour le champ, entrez le type de résultat de votre action de script vRealize Orchestrator.
Paramètre d'entrée	Si vous utilisez le champ pour accepter la saisie du consommateur et transmettre les paramètres à vRealize Orchestrator, entrez le type de paramètre d'entrée accepté par le workflow vRealize Orchestrator.
Paramètre de sortie	Si vous utilisez le champ pour afficher des informations pour les consommateurs, entrez le type de paramètre de sortie du workflow vRealize Orchestrator.

- 9 (Facultatif) Cochez la case **Valeurs multiples** pour permettre aux consommateurs de sélectionner plusieurs objets.

Cette option n'est pas disponible pour tous les types de champs.

- 10 Cliquez sur **Envoyer**.

- 11 Cliquez sur **Terminer**.

Suivant

Vous pouvez modifier l'élément afin de changer les paramètres par défaut et appliquer diverses contraintes ou valeurs.


Modifier un élément d'action sur la ressource

Vous pouvez modifier certaines des caractéristiques d'un élément sur la page Formulaire d'action sur la ressource. Vous pouvez modifier le type d'un élément, ses valeurs par défaut, et appliquer différentes contraintes et valeurs.

Prérequis

- Connectez-vous à la console vRealize Automation en tant **qu'administrateur de locataire** ou **architecte XaaS**.
- [Créer une action sur les ressources](#).

Procédure

- 1 Sélectionnez **Conception > XaaS > Actions sur les ressources**.
- 2 Cliquez sur l'action sur la ressource à modifier.
- 3 Cliquez sur l'onglet **Formulaire**.
- 4 Cliquez sur l'élément à modifier.
- 5 Cliquez sur l'icône **Modifier** ()
- 6 Entrez un nouveau nom pour le champ dans la zone de texte **Étiquette** pour modifier l'étiquette que les consommateurs voient.

- 7 Modifiez la description dans la zone de texte **Description**.
- 8 Sélectionnez une option dans le menu déroulant **Type** pour modifier le type d'affichage de l'élément.
Les options varient en fonction du type d'élément que vous modifiez.
- 9 Sélectionnez une option dans le menu déroulant **Taille** pour modifier la taille de l'élément.
- 10 Sélectionnez une option dans le menu déroulant **Taille d'étiquette** pour modifier la taille de l'étiquette.
- 11 Modifiez la valeur par défaut de l'élément.

Option	Description
Non définie	Obtient la valeur de l'élément que vous modifiez dans la présentation du workflow vRealize Orchestrator.
Constante	Définit la valeur par défaut de l'élément que vous modifiez dans une valeur constante que vous spécifiez.
Champ	Lie la valeur par défaut de l'élément à un paramètre d'un autre élément de la représentation.
Conditionnelle	Applique une condition. En utilisant des conditions, vous pouvez créer plusieurs clauses et expressions, puis les appliquer à un élément.
Externe	Sélectionnez une action de script vRealize Orchestrator pour définir la valeur.

- 12 Appliquer des contraintes à l'élément dans l'onglet **Contraintes**.

Option	Description
Non définie	Obtient la valeur de l'élément que vous modifiez dans la présentation du workflow vRealize Orchestrator.
Constante	Définit la valeur par défaut de l'élément que vous modifiez dans une valeur constante que vous spécifiez.
Champ	Lie la valeur par défaut de l'élément à un paramètre d'un autre élément de la représentation.
Conditionnelle	Applique une condition. En utilisant des conditions, vous pouvez créer plusieurs clauses et expressions, puis les appliquer à un élément.
Externe	Sélectionnez une action de script vRealize Orchestrator pour définir la valeur.

- 13 Ajouter une ou plusieurs valeurs à l'élément dans l'onglet **Valeurs**.

Les options disponibles varient en fonction du type d'élément que vous modifiez.

Option	Description
Non définie	Obtient la valeur de l'élément que vous modifiez dans la présentation du workflow vRealize Orchestrator.
Valeurs prédéfinies	<p>Sélectionnez les valeurs dans une liste d'objets associés dans l'inventaire vRealize Orchestrator.</p> <ol style="list-style-type: none"> a Entrez une valeur dans la zone de recherche Valeurs prédéfinies pour rechercher l'inventaire vRealize Orchestrator. b Sélectionnez une valeur dans les résultats de la recherche et appuyez sur Entrée.

Option	Description
Valeur	Définissez des valeurs personnalisées avec des étiquettes. a Entrez une valeur dans la zone de texte Valeur . b Entrez une étiquette pour la valeur dans la zone de texte Étiquette . c Cliquez sur l'icône Ajouter (+).
Valeurs externes	Sélectionnez une action de script vRealize Orchestrator pour définir votre valeur avec des informations qui ne sont pas directement exposées par le workflow. <ul style="list-style-type: none"> ■ Sélectionnez Ajouter une valeur externe. ■ Sélectionnez votre action de script vRealize Orchestrator. ■ Cliquez sur Soumettre.

14 Cliquez sur **Envoyer**.

15 Cliquez sur **Mise à jour**.

Insérer un en-tête de section dans un formulaire d'action sur la ressource

Vous pouvez insérer un en-tête de section pour diviser le formulaire en sections.

Prérequis

- Connectez-vous à la console vRealize Automation en tant **qu'administrateur de locataire** ou **architecte XaaS**.
- [Créer une action sur les ressources](#).

Procédure

- 1 Sélectionnez **Conception > XaaS > Actions sur les ressources**.
- 2 Cliquez sur l'action sur la ressource à modifier.
- 3 Cliquez sur l'onglet **Formulaire**.
- 4 Faites glisser l'élément **En-tête de section** du panneau Formulaire vers le panneau de la page Formulaire.
- 5 Tapez un nom pour la section.
- 6 Cliquez en dehors de l'élément pour enregistrer les modifications.
- 7 Cliquez sur **Terminer**.

Ajouter un élément de texte à un formulaire d'action sur les ressources

Vous pouvez insérer une zone de texte afin d'ajouter des observations descriptives au formulaire.

Prérequis

- Connectez-vous à la console vRealize Automation en tant **qu'administrateur de locataire** ou **architecte XaaS**.
- [Créer une action sur les ressources](#).

Procédure

- 1 Sélectionnez **Conception > XaaS > Actions sur les ressources**.
- 2 Cliquez sur l'action sur la ressource à modifier.
- 3 Cliquez sur l'onglet **Formulaire**.
- 4 Faites glisser l'élément **Texte** du panneau Nouveaux champs vers le panneau de la page Formulaire.
- 5 Entrez le texte à ajouter.
- 6 Cliquez en dehors de l'élément pour enregistrer les modifications.
- 7 Cliquez sur **Terminer**.

Exemples et scénarios XaaS

Les exemples et scénarios suggèrent des utilisations de vRealize Automation afin de réaliser les tâches courantes à l'aide des Blueprints XaaS et des actions sur la ressource.

Créer un Blueprint XaaS ainsi qu'une action visant à créer et à modifier un utilisateur

XaaS vous permet de créer et de publier un élément du catalogue afin de provisionner l'utilisateur d'un groupe. Vous pouvez également associer une nouvelle opération de post-provisionnement à l'utilisateur provisionné. Par exemple, une opération permettant aux utilisateurs du catalogue de services de modifier le mot de passe utilisateur.

En tant qu'architecte XaaS, créez une ressource personnalisée, un Blueprint XaaS et publiez un élément du catalogue pour la création d'un utilisateur. Vous pouvez également créer une action sur la ressource visant à modifier le mot de passe de l'utilisateur.

En tant qu'administrateur du catalogue, créez un service et incluez-y l'élément du catalogue Blueprint. De plus, modifiez la présentation du workflow de l'élément du catalogue à l'aide du concepteur de formulaires et changez la façon dont les consommateurs voient le formulaire de demande.

En tant que gestionnaire de groupe d'activité ou administrateur de locataire, accordez à un consommateur un droit d'accès au service, à l'élément de catalogue et à l'action sur la ressource que vous venez de créer.

Prérequis

Vérifiez que le plug-in Active Directory est correctement configuré et que vous disposez des droits permettant de créer des utilisateurs dans Active Directory.

Procédure

1 Créer un utilisateur test en tant que ressource personnalisée

Vous pouvez créer une ressource personnalisée et la mapper au type d'objet vRealize Orchestrator AD:User.

2 Créer un Blueprint XaaS pour la création d'un utilisateur

Créez le Blueprint XaaS Créer un utilisateur dans un groupe afin de pouvoir exécuter le workflow qui ajoute un utilisateur Active Directory et attribue cet utilisateur à un groupe Active Directory. Vous pouvez créer le Blueprint XaaS en tant que Blueprint autonome ou composant de Blueprint. Dans ce scénario, vous créez un Blueprint autonome.

3 Créez une action sur les ressources pour modifier un mot de passe d'utilisateur

Vous pouvez créer une action sur les ressources pour permettre aux consommateurs de l'instance de XaaS de modifier le mot de passe de l'utilisateur après avoir provisionné ce dernier.

4 Créer un service et ajouter le Blueprint Créer un utilisateur test au service

Vous pouvez créer un service pour afficher l'élément Créer un utilisateur dans le catalogue de services.

5 Autoriser le service et l'action sur la ressource pour un consommateur

Les gestionnaires de groupes d'activité et les gestionnaires de locataires peuvent autoriser un utilisateur ou un groupe d'utilisateurs à accéder au service ou à l'action sur la ressource. Une fois autorisés, ils peuvent afficher le service dans leur catalogue et demander l'élément du catalogue Créer un utilisateur test qui est inclus dans le service. Une fois que les consommateurs ont provisionné l'élément, ils peuvent demander la modification du mot de passe.

Créer un utilisateur test en tant que ressource personnalisée

Vous pouvez créer une ressource personnalisée et la mapper au type d'objet vRealize Orchestrator AD:User.

Prérequis

Connectez-vous à la console vRealize Automation en tant qu'**architecte XaaS**.

Procédure

- 1 Sélectionnez **Conception > XaaS > Ressources personnalisées**.
- 2 Cliquez sur l'icône **Nouveau (+)**.
- 3 Dans la zone de texte **Type de la variable dans l'orchestrateur**, entrez **AD:User** et appuyez sur Entrée.
- 4 Sélectionnez **AD:User** dans la liste.
- 5 Tapez un nom pour la ressource.
Par exemple, **Utilisateur test**.
- 6 Entrez une description pour la ressource.
Par exemple,
Il s'agit d'une ressource test personnalisée que j'utiliserai pour mon élément de catalogue afin de créer un utilisateur dans un groupe.
- 7 Cliquez sur **Suivant**.

8 Conservez les valeurs par défaut dans le formulaire.

9 Cliquez sur **Terminer**.

Vous avez créé une ressource personnalisée Utilisateur test et vous pouvez la voir sur la page Ressources personnalisées.

Suivant

Créez un Blueprint XaaS.

Créer un Blueprint XaaS pour la création d'un utilisateur

Créez le Blueprint XaaS Créer un utilisateur dans un groupe afin de pouvoir exécuter le workflow qui ajoute un utilisateur Active Directory et attribue cet utilisateur à un groupe Active Directory. Vous pouvez créer le Blueprint XaaS en tant que Blueprint autonome ou composant de Blueprint. Dans ce scénario, vous créez un Blueprint autonome.

Prérequis

- Assurez-vous que vous créez une action sur la ressource personnalisée qui prenne en charge le provisionnement des utilisateurs d'Active Directory. Reportez-vous à [Créer un utilisateur test en tant que ressource personnalisée](#).
- Connectez-vous à la console vRealize Automation en tant qu'**architecte XaaS**.

Procédure

- 1 Sélectionnez **Conception > XaaS > Blueprints XaaS**.
- 2 Cliquez sur l'icône **Nouveau (+)**.
- 3 Dans le volet Sélectionner un workflow, accédez à **Orchestrator > Bibliothèque > Microsoft > Active Directory > Utilisateur** et sélectionnez le workflow **Créer un utilisateur dans un groupe**.
- 4 Cliquez sur **Suivant**.
- 5 Configurez les options de l'onglet **Général**.
 - a Remplacez le nom du Blueprint par **Créer un utilisateur test** et laissez la description telle quelle.
 - b Décochez la case **Rendre disponible comme composant dans le canevas de conception**.
 Au lieu de l'utiliser en tant que composant de Blueprint dans le canevas de conception, vous publiez ce Blueprint directement dans le catalogue de conception. Il n'est pas nécessaire de configurer des workflows de réduction de charge ou de montée en charge.
 L'onglet **Cycle de vie du composant** est supprimé de l'interface utilisateur.
- 6 Cliquez sur **Suivant**.

7 Modifiez le formulaire de Blueprint.

- a Cliquez sur **Le nom de domaine dans le format Win2000**.
- b Cliquez sur l'onglet **Contraintes**.
- c Cliquez sur la flèche de déroulement **Valeur**, sélectionnez **Constante** dans le menu déroulant, puis entrez **test.domain**.
- d Cliquez sur la flèche de déroulement **Visible**, sélectionnez **Constante** dans le menu déroulant, puis sélectionnez **Non** dans le menu déroulant.

Vous avez rendu le nom de domaine invisible au consommateur de l'élément du catalogue.

- e Cliquez sur **Appliquer** pour enregistrer les modifications.

8 Cliquez sur **Suivant**.

9 Sélectionnez **NouvelUtilisateur [Utilisateur test]** comme paramètre de sortie pour être provisionné.

10 Cliquez sur **Suivant**.

11 Cliquez sur **Terminer**.

12 Sur la page **Blueprints XaaS**, sélectionnez la ligne **Créer un utilisateur de test** et cliquez sur **Publier**.

Vous avez créé un Blueprint de création d'un utilisateur test et vous avez rendu le Blueprint disponible pour l'ajouter à un service.

Suivant

Créez une action à exécuter sur le compte d'utilisateur provisionné. Reportez-vous à [Créez une action sur les ressources pour modifier un mot de passe d'utilisateur](#).

Créez une action sur les ressources pour modifier un mot de passe d'utilisateur

Vous pouvez créer une action sur les ressources pour permettre aux consommateurs de l'instance de XaaS de modifier le mot de passe de l'utilisateur après avoir provisionné ce dernier.

Prérequis

- Connectez-vous à la console vRealize Automation en tant qu'**architecte XaaS**.
- Assurez-vous que vous créez une action sur la ressource personnalisée qui prenne en charge le provisionnement des utilisateurs d'Active Directory. Reportez-vous à [Créer un utilisateur test en tant que ressource personnalisée](#).

Procédure

- 1 Sélectionnez **Conception > XaaS > Actions sur les ressources**.
- 2 Cliquez sur l'icône **Nouveau (+)**.

- 3 Accédez à **Orchestrator > Bibliothèque > Microsoft > Active Directory > Utilisateur** dans la bibliothèque de workflows vRealize Orchestrator et sélectionnez le workflow **Modifier un mot de passe utilisateur**.
- 4 Cliquez sur **Suivant**.
- 5 Sélectionnez **Utilisateur test** dans le menu déroulant **Type de ressource**.
Cette sélection représente la ressource personnalisée que vous avez créée précédemment.
- 6 Sélectionnez **utilisateur** dans le menu déroulant **Paramètre d'entrée**.
- 7 Cliquez sur **Suivant**.
- 8 Modifiez le nom de l'action sur les ressources par **Modifier le mot de passe de l'utilisateur test** et laissez la description telle qu'elle s'affiche dans l'onglet **Détails**.
- 9 Cliquez sur **Suivant**.
- 10 (Facultatif) Laissez le formulaire tel quel.
- 11 Cliquez sur **Terminer**.
- 12 Sur la page Actions sur la ressource, sélectionnez la ligne **Modifier le mot de passe de l'utilisateur test** et cliquez sur **Publier**.

Vous avez créé une action sur la ressource pour modifier le mot de passe d'un utilisateur et vous l'avez rendue disponible pour l'ajouter à un droit.

Suivant

Ajoutez le Blueprint Créer un utilisateur test à un service. Reportez-vous à [Créer un service et ajouter le Blueprint Créer un utilisateur test au service](#).

Créer un service et ajouter le Blueprint Créer un utilisateur test au service

Vous pouvez créer un service pour afficher l'élément Créer un utilisateur dans le catalogue de services.

Prérequis

- Connectez-vous à la console vRealize Automation en tant qu'**administrateur de locataire** ou **administrateur de catalogue**.
- Vérifiez que vous avez créé un Blueprint XaaS. Reportez-vous à [Créer un Blueprint XaaS pour la création d'un utilisateur](#).

Connectez-vous à la console vRealize Automation en tant qu'**administrateur de locataire** ou **administrateur de catalogue**.

Procédure

- 1 Sélectionnez **Administration > Gestion de catalogue > Services**.
- 2 Cliquez sur l'icône **Nouveau (+)**.

- 3 Entrez **Créer un utilisateur test Active Directory** comme nom du service.
- 4 Sélectionnez **Actif** dans le menu déroulant **Statut**.
- 5 Laissez les autres zones de texte vides.
- 6 Cliquez sur **OK**.
- 7 Dans la liste Services, sélectionnez la ligne **Créer un utilisateur test Active Directory** et cliquez sur **Gérer les éléments du catalogue**.
- 8 Cliquez sur l'icône **Nouveau (+)**.
- 9 Sélectionnez **Créer un utilisateur test**, puis cliquez sur **OK**.
Le Blueprint Créer un utilisateur test XaaS s'ajoute à la liste d'éléments du catalogue.
- 10 Cliquez sur **Fermer**.

Le service Créer un utilisateur test Active Directory inclut désormais le Blueprint Créer un utilisateur test. Il n'est pas nécessaire d'ajouter des actions à des services.

Suivant

Vous pouvez autoriser les utilisateurs à demander le Blueprint et exécuter l'action. Reportez-vous à [Autoriser le service et l'action sur la ressource pour un consommateur](#).

Autoriser le service et l'action sur la ressource pour un consommateur

Les gestionnaires de groupes d'activité et les gestionnaires de locataires peuvent autoriser un utilisateur ou un groupe d'utilisateurs à accéder au service ou à l'action sur la ressource. Une fois autorisés, ils peuvent afficher le service dans leur catalogue et demander l'élément du catalogue Créer un utilisateur test qui est inclus dans le service. Une fois que les consommateurs ont provisionné l'élément, ils peuvent demander la modification du mot de passe.

Prérequis

- Connectez-vous à la console vRealize Automation en tant qu'**administrateur de locataire** ou **gestionnaire de groupes d'activités**.
- Assurez-vous que le Blueprint Créer un utilisateur est ajouté à un service. Reportez-vous à [Créer un service et ajouter le Blueprint Créer un utilisateur test au service](#).
- Assurez-vous que l'action sur la ressource Modifier un mot de passe d'utilisateur existe. Reportez-vous à [Créer une action sur les ressources pour modifier un mot de passe d'utilisateur](#).

Procédure

- 1 Sélectionnez **Administration > Gestion de catalogue > Droits d'accès**.
- 2 Cliquez sur l'icône **Nouveau (+)**.
- 3 Entrez **Créer un utilisateur Active Directory** dans la zone de texte **Nom**.
- 4 Laissez les zones de texte **Description** et **Date d'expiration** vides.

- 5 Sélectionnez **Actif** dans le menu déroulant **Statut**.
- 6 Sélectionnez un groupe d'activité cible dans le menu déroulant **Groupe d'activité**.
Par exemple, gestionnaire de compte informatique.
- 7 Sélectionnez **Tous les utilisateurs et groupes** pour autoriser tous les membres du groupe d'activité, les gestionnaires de compte informatique par exemple, à créer un compte d'utilisateur.

Les utilisateurs que vous sélectionnez peuvent afficher le service et les éléments du catalogue inclus dans le service dans le catalogue. Ils peuvent exécuter l'action Modifier le mot de passe sur le compte d'utilisateur une fois qu'il a été créé.
- 8 Cliquez sur **Suivant**.
- 9 Dans la zone de texte **Services autorisés**, entrez **Utilisateur test Active Directory** et appuyez sur la touche Entrée.
- 10 Dans la zone de texte **Actions autorisées**, entrez **Modifier le mot de passe de l'utilisateur test** et appuyez sur la touche Entrée.
- 11 Cliquez sur **Terminer**.

Vous avez créé un droit d'accès actif autorisant les utilisateurs qui sont membres du groupe d'activité Gestionnaires de compte informatique à créer des utilisateurs. Une fois l'utilisateur provisionné, ils peuvent exécuter l'action sur la ressource Modifier le mot de passe de l'utilisateur sur le compte d'utilisateur provisionné.

Suivant

Connectez-vous en tant qu'utilisateur autorisé à créer un utilisateur Active Directory. Dans l'onglet **Catalogue**, vérifiez que le Blueprint XaaS crée l'utilisateur comme prévu. Une fois l'utilisateur créé, exécutez l'action Modifier le mot de passe depuis l'onglet **Éléments**.

Créer et publier une action XaaS pour migrer une machine virtuelle

Vous pouvez créer et publier une action sur la ressource XaaS afin d'étendre les opérations que les consommateurs peuvent exécuter sur des machines virtuelles vSphere provisionnées avec IaaS.

Dans ce scénario, créez une action sur la ressource pour migrer rapidement une machine virtuelle vSphere.

Prérequis

Connectez-vous à la console vRealize Automation en tant qu'**architecte XaaS**.

Procédure

1 Créer une action sur les ressources pour migrer une machine virtuelle vSphere

Vous pouvez créer une action personnalisée sur les ressources pour permettre aux consommateurs de migrer des machines virtuelles vSphere après avoir provisionnées les machines virtuelles vSphere avec IaaS.

2 [Publier l'action pour la migration d'une machine virtuelle vSphere](#)

Pour utiliser l'action sur la ressource Migration rapide d'une machine virtuelle comme opération post-provisionnement, vous devez la publier.

Créer une action sur les ressources pour migrer une machine virtuelle vSphere

Vous pouvez créer une action personnalisée sur les ressources pour permettre aux consommateurs de migrer des machines virtuelles vSphere après avoir provisionnées les machines virtuelles vSphere avec IaaS.

Procédure

- 1 Sélectionnez **Conception > XaaS > Actions sur les ressources**.
- 2 Cliquez sur **Ajouter (+)**.
- 3 Accédez à **Orchestrator > Bibliothèque > vCenter > Gestion des machines virtuelles > Déplacer et migrer** dans la bibliothèque de workflows vRealize Orchestrator et sélectionnez le workflow **Migration rapide de machine virtuelle**.
- 4 Cliquez sur **Suivant**.
- 5 Sélectionnez **IaaS VC VirtualMachine** dans le menu déroulant **Type de ressources**.
- 6 Sélectionnez **vm** dans le menu déroulant **Paramètre d'entrée**.
- 7 Cliquez sur **Suivant**.
- 8 Laissez le nom et la description de l'action sur les ressources tels qu'ils s'affichent dans l'onglet **Détails**.
- 9 Cliquez sur **Suivant**.
- 10 Laissez le formulaire tel quel.
- 11 Cliquez sur **Terminer**.

Vous avez créé une action sur les ressources pour migrer une machine virtuelle et vous pouvez la voir apparaître sur la page Actions sur les ressources.

Suivant

[Publier l'action pour la migration d'une machine virtuelle vSphere](#)

Publier l'action pour la migration d'une machine virtuelle vSphere

Pour utiliser l'action sur la ressource Migration rapide d'une machine virtuelle comme opération post-provisionnement, vous devez la publier.

Procédure

- 1 Sélectionnez **Conception > XaaS > Actions sur les ressources**.
- 2 Sélectionnez la ligne de l'action sur la ressource Migration rapide d'une machine virtuelle et cliquez sur le bouton **Publier**.

Vous avez créé et publié un workflow vRealize Orchestrator en tant qu'action sur les ressources. Vous pouvez accéder à **Administration > Gestion de catalogues > Actions** et voir l'action sur les ressources Migration rapide de la machine virtuelle dans la liste des actions. Vous pouvez attribuer une icône à l'action sur les ressources. Reportez-vous à [Attribuer une icône à une action sur les ressources XaaS](#).

Suivant

Ajoutez l'action aux droits d'accès qui contiennent les machines virtuelles vSphere provisionnées par IaaS. Reportez-vous à [Autoriser des utilisateurs à accéder à des services, des éléments de catalogue et des actions](#).

Créer une action XaaS pour migrer une machine virtuelle avec vMotion

XaaS vous permet de créer et de publier une action sur la ressource visant à migrer, à l'aide de vMotion, une machine virtuelle provisionnée avec IaaS.

Dans ce scénario, créez une action sur la ressource afin de migrer une machine virtuelle vSphere avec vMotion. De plus, modifiez la présentation du workflow à l'aide du concepteur de formulaires et changez l'affichage de l'action pour les consommateurs lorsqu'ils la demandent.

Prérequis

Connectez-vous à la console vRealize Automation en tant qu'**architecte XaaS**.

Procédure

1 [Créer une action pour migrer une machine virtuelle vSphere avec vMotion](#)

Vous pouvez créer une action personnalisée sur la ressource pour permettre aux utilisateurs du catalogue de services de migrer une machine virtuelle vSphere avec vMotion après l'avoir provisionnée avec IaaS.

2 [Modifier le formulaire d'action sur la ressource](#)

Le formulaire d'action sur la ressource mappe la présentation du workflow vRealize Orchestrator. Vous pouvez éditer le formulaire et définir ce que les consommateurs de l'action sur la ressource voient lorsqu'ils décident d'exécuter l'opération de post-provisionnement.

3 [Ajouter un formulaire de détails d'action envoyée et enregistrer l'action](#)

Vous pouvez ajouter un nouveau formulaire à l'action de ressource Migrer une machine virtuelle avec vMotion pour déterminer ce que les utilisateurs voient après avoir demandé d'exécuter l'opération de post-provisionnement.

4 [Publier l'action pour la migration d'une machine virtuelle avec vMotion](#)

Pour utiliser l'action sur la ressource Migrer une machine virtuelle avec vMotion comme opération post-provisionnement, vous devez la publier.

Créer une action pour migrer une machine virtuelle vSphere avec vMotion

Vous pouvez créer une action personnalisée sur la ressource pour permettre aux utilisateurs du catalogue de services de migrer une machine virtuelle vSphere avec vMotion après l'avoir provisionnée avec IaaS.

Procédure

- 1 Sélectionnez **Conception > XaaS > Actions sur les ressources**.
- 2 Cliquez sur **Ajouter** (+).
- 3 Accédez à **Orchestrator > Bibliothèque > vCenter > Gestion des machines virtuelles > Déplacer et migrer** dans la bibliothèque de workflows vRealize Orchestrator et sélectionnez le workflow **Migrer la machine virtuelle avec vMotion**.
- 4 Cliquez sur **Suivant**.
- 5 Sélectionnez **IaaS VC VirtualMachine** dans le menu déroulant **Type de ressources**.
- 6 Sélectionnez **vm** dans le menu déroulant **Paramètre d'entrée**.
- 7 Cliquez sur **Suivant**.
- 8 Laissez le nom et la description de l'action sur les ressources tels qu'ils s'affichent dans l'onglet **Détails**.
- 9 Cliquez sur **Suivant**.

Suivant

Reportez-vous à [Modifier le formulaire d'action sur la ressource](#).

Modifier le formulaire d'action sur la ressource

Le formulaire d'action sur la ressource mappe la présentation du workflow vRealize Orchestrator. Vous pouvez éditer le formulaire et définir ce que les consommateurs de l'action sur la ressource voient lorsqu'ils décident d'exécuter l'opération de post-provisionnement.


Procédure

- 1 Cliquez sur l'icône **Supprimer** (✖) pour supprimer l'élément **pool**.
- 2 Modifiez l'élément **hôte**.
 - a Cliquez sur l'icône **Modifier** (✎) située en regard du champ **hôte**.
 - b Dans la zone de texte **Étiquette**, saisissez **Hôte cible**.
 - c Dans le menu déroulant **Type**, sélectionnez **Rechercher**.
 - d Cliquez sur l'onglet **Contraintes**.
 - e Dans le menu déroulant **Requis**, sélectionnez **Constante** et sélectionnez **Oui**.
Le champ hôte est maintenant toujours requis.
 - f Cliquez sur **Envoyer**.
- 3 Modifiez l'élément **priorité**.
 - a Cliquez sur l'icône **Modifier** (✎) située en regard du champ **priorité**.
 - b Saisissez **Priorité de la tâche** dans la zone de texte **Étiquette**.

- c Dans le menu déroulant **Type**, sélectionnez **Groupe de boutons radio**.
- d Cliquez sur l'onglet **Valeurs** et décochez la case **Non définies**.
- e Dans la zone de texte de recherche **Valeurs prédéfinies**, saisissez **Priorité faible**, puis appuyez sur la touche Entrée.
- f Dans la zone de texte de recherche **Valeurs prédéfinies**, saisissez **Priorité par défaut**, puis appuyez sur la touche Entrée.
- g Dans la zone de texte de recherche **Valeurs prédéfinies**, saisissez **Priorité élevée**, puis appuyez sur la touche Entrée.
- h Cliquez sur **Envoyer**.

Lorsque les consommateurs demandent l'action sur la ressource, un groupe de trois boutons radio apparaît : **Priorité faible**, **Priorité par défaut** et **Priorité élevée**.

4 Modifiez l'élément **État**.

- a Cliquez sur l'icône **Modifier** () située en regard du champ **État**.
- b Dans la zone de texte **Étiquette**, saisissez **État de la machine virtuelle**.
- c Dans le menu déroulant **Type**, sélectionnez **Liste déroulante**.
- d Cliquez sur l'onglet **Valeurs** et décochez la case **Non définies**.
- e Dans la zone de texte de recherche **Valeurs prédéfinies**, saisissez **Hors tension**, puis appuyez sur la touche Entrée.
- f Dans la zone de texte de recherche **Valeurs prédéfinies**, saisissez **Sous tension**, puis appuyez sur la touche Entrée.
- g Dans la zone de texte de recherche **Valeurs prédéfinies**, saisissez **Interrompu**, puis appuyez sur la touche Entrée.
- h Cliquez sur **Envoyer**.

Lorsque les consommateurs demandent l'action sur la ressource, un menu déroulant apparaît avec les trois options : **Hors tension**, **Sous tension** et **Interrompu**.

Vous avez modifié la présentation de workflow de la machine virtuelle Migrer avec le workflow vMotion.

Suivant

[Ajouter un formulaire de détails d'action envoyée et enregistrer l'action.](#)

Ajouter un formulaire de détails d'action envoyée et enregistrer l'action

Vous pouvez ajouter un nouveau formulaire à l'action de ressource Migrer une machine virtuelle avec vMotion pour déterminer ce que les utilisateurs voient après avoir demandé d'exécuter l'opération de post-provisionnement.

Procédure

- 1 Cliquez sur l'icône **Nouveau formulaire** (+) en regard du menu déroulant **Formulaire**.
- 2 Tapez **Action soumise** dans la zone de texte **Nom**.
- 3 Laissez le champ **Description** vide.
- 4 Sélectionnez **Détails de l'action soumise** dans le menu **Type d'écran**.
- 5 Cliquez sur **Envoyer**.
- 6 Cliquez sur l'icône **Modifier** (✎) en regard du menu déroulant **Page de formulaire**.
- 7 Tapez **Détails** dans la zone de texte **En-tête**.
- 8 Cliquez sur **Envoyer**.
- 9 Faites glisser l'élément **Texte** du panneau Formulaire et déposez-le sur la page **Formulaire**.
- 10 Tapez
Vous avez envoyé une demande pour migrer votre machine avec vMotion. Patientez jusqu'à la fin du processus.
- 11 Cliquez en dehors de la zone de texte pour enregistrer les modifications.
- 12 Cliquez sur **Envoyer**.
- 13 Cliquez sur **Ajouter**.

Vous avez créé une action sur les ressources pour migrer une machine virtuelle avec vMotion et vous pouvez la voir apparaître sur la page Actions sur les ressources.

Suivant

[Publier l'action pour la migration d'une machine virtuelle avec vMotion.](#)

Publier l'action pour la migration d'une machine virtuelle avec vMotion

Pour utiliser l'action sur la ressource Migrer une machine virtuelle avec vMotion comme opération post-provisionnement, vous devez la publier.

Procédure

- 1 Sélectionnez **Conception > XaaS > Actions sur les ressources**.
- 2 Sélectionnez la ligne de l'action Migrer une machine virtuelle avec vMotion et cliquez sur le bouton **Publier**.

Vous avez créé et publié un workflow vRealize Orchestrator en tant qu'action sur les ressources. Vous pouvez accéder à **Administration > Gestion de catalogues > Actions** et voir l'action sur les ressources Migrer une machine virtuelle avec vMotion dans la liste des actions. Vous pouvez attribuer une icône à l'action sur les ressources. Reportez-vous à [Attribuer une icône à une action sur les ressources XaaS](#).

Vous avez également modifié la présentation du workflow et défini l'apparence de l'action.

Suivant

Les gestionnaires de groupes d'activités et les gestionnaires de locataires peuvent inclure l'action sur les ressources Migrer une machine virtuelle avec vMotion dans une autorisation. Pour plus d'informations sur la création et la publication de Blueprints IaaS pour plates-formes virtuelles, reportez-vous à [Conception de Blueprints de machine](#).

Créer et publier une action XaaS pour prendre un snapshot

XaaS vous permet de créer et de publier une action sur la ressource visant à prendre un snapshot d'une machine virtuelle vSphere provisionnée avec IaaS.

Dans ce scénario, créez une action sur la ressource afin de prendre un snapshot d'une machine virtuelle vSphere provisionnée avec IaaS. De plus, modifiez la présentation du workflow à l'aide du concepteur de formulaires et changez l'affichage de l'action pour les consommateurs lorsqu'ils la demandent.

Prérequis

Connectez-vous à la console vRealize Automation en tant qu'**architecte XaaS**.

Procédure

1 Créer une action pour prendre un snapshot d'une machine virtuelle vSphere

Vous pouvez créer une action personnalisée sur une ressource pour permettre aux consommateurs de prendre un snapshot d'une machine virtuelle vSphere après l'avoir provisionnée avec IaaS.

2 Publier l'action pour la prise d'un snapshot

Pour utiliser l'action sur la ressource Créer un snapshot comme opération post-provisionnement, vous devez la publier.

Créer une action pour prendre un snapshot d'une machine virtuelle vSphere

Vous pouvez créer une action personnalisée sur une ressource pour permettre aux consommateurs de prendre un snapshot d'une machine virtuelle vSphere après l'avoir provisionnée avec IaaS.

Procédure

- 1 Sélectionnez **Conception > XaaS > Actions sur les ressources**.
- 2 Cliquez sur **Ajouter** (+).
- 3 Accédez à **Orchestrator > Bibliothèque > vCenter > Gestion des machines virtuelles > Snapshot** dans la bibliothèque de workflows vRealize Orchestrator et sélectionnez le workflow **Créer un snapshot**.
- 4 Cliquez sur **Suivant**.
- 5 Sélectionnez **IaaS VC VirtualMachine** dans le menu déroulant **Type de ressources**.
- 6 Sélectionnez **vm** dans le menu déroulant **Paramètre d'entrée**.
- 7 Cliquez sur **Suivant**.
- 8 Laissez le nom et la description de l'action sur les ressources tels qu'ils s'affichent dans l'onglet **Détails**.

9 Cliquez sur **Suivant**.

10 Laissez le formulaire tel quel.

11 Cliquez sur **Ajouter**.

Vous avez créé une action sur la ressource pour prendre un snapshot d'une machine virtuelle, qui apparaît sur la page Actions sur les ressources.

Suivant

[Publier l'action pour la prise d'un snapshot.](#)

Publier l'action pour la prise d'un snapshot

Pour utiliser l'action sur la ressource Créer un snapshot comme opération post-provisionnement, vous devez la publier.

Procédure

- 1 Sélectionnez **Conception > XaaS > Actions sur les ressources**.
- 2 Sélectionnez la ligne de l'action Créer un snapshot et cliquez sur le bouton **Publier**.

Vous avez créé et publié un workflow vRealize Orchestrator en tant qu'action sur les ressources. Vous pouvez accéder à **Administration > Gestion de catalogues > Actions** et voir l'action sur les ressources Créer un snapshot dans la liste des actions. Vous pouvez attribuer une icône à l'action sur les ressources. Reportez-vous à [Attribuer une icône à une action sur les ressources XaaS](#).

Suivant

Les gestionnaires de groupes d'activités et les gestionnaires de locataires peuvent inclure l'action sur les ressources Créer un snapshot dans une autorisation. Pour plus d'informations sur la création et la publication de Blueprints IaaS pour plates-formes virtuelles, reportez-vous à [Conception de Blueprints de machine](#).

Créer et publier une action XaaS pour démarrer une machine virtuelle Amazon

XaaS vous permet de créer et de publier des actions visant à étendre les opérations exécutées par les consommateurs sur des ressources provisionnées tierces.

Dans ce scénario, créez et publiez une action sur la ressource pour démarrer rapidement les machines virtuelles Amazon.

Prérequis

- Installez le plug-in vRealize Orchestrator des services Web Amazon sur le serveur vRealize Orchestrator par défaut.
- Créez ou importez un workflow vRealize Orchestrator pour le mappage de la ressource des instances d'Amazon.

Procédure

1 Créer un mappage de ressources pour les instances Amazon

Vous pouvez créer un mappage de ressources afin d'associer des instances d'Amazon provisionnées à l'aide IaaS avec le type vRealize Orchestrator AWS:EC2Instance exposé par le plug-in des services Web Amazon.

2 Créer une action sur les ressources pour démarrer une machine virtuelle Amazon

Vous pouvez créer une action sur les ressources de sorte que les consommateurs puissent démarrer des machines virtuelles Amazon.

3 Publier l'action pour le démarrage des instances d'Amazon

Pour utiliser l'action sur la ressource Démarrer des instances créée récemment pour le des opérations de post-provisionnement sur des machines virtuelles Amazon, vous devez la publier.

Créer un mappage de ressources pour les instances Amazon

Vous pouvez créer un mappage de ressources afin d'associer des instances d'Amazon provisionnées à l'aide IaaS avec le type vRealize Orchestrator AWS:EC2Instance exposé par le plug-in des services Web Amazon.

Prérequis

- Connectez-vous à la console vRealize Automation en tant qu'**architecte XaaS**.
- Créez ou importez un workflow de mappage de ressources ou une action de script vRealize Orchestrator.

Procédure

- 1 Sélectionnez **Conception > XaaS > Mappage de ressource**.
- 2 Cliquez sur **Ajouter** (+).
- 3 Entrez **Instance EC2** dans la zone de texte **Nom**.
- 4 Entrez **Machine Cloud** dans la zone de texte **Type de ressources du catalogue**.
- 5 Entrez **AWS:EC2Instance** dans la zone de texte **Type d'Orchestrator**.
- 6 Sélectionnez **Toujours disponible**.
- 7 Sélectionnez le type de mappage de ressources à utiliser.
- 8 Sélectionnez l'action de script ou le workflow de votre mappage de ressources personnalisées dans la bibliothèque vRealize Orchestrator.
- 9 Cliquez sur **Ajouter**.

Vous pouvez utiliser votre mappage de ressources Amazon pour créer des actions sur les ressources pour les machines Amazon provisionnées à l'aide d'IaaS.

Suivant

[Créer une action sur les ressources pour démarrer une machine virtuelle Amazon.](#)

Créer une action sur les ressources pour démarrer une machine virtuelle Amazon

Vous pouvez créer une action sur les ressources de sorte que les consommateurs puissent démarrer des machines virtuelles Amazon.

Prérequis

Connectez-vous à la console vRealize Automation en tant qu'**architecte XaaS**.

Procédure

- 1 Sélectionnez **Conception > XaaS > Actions sur les ressources**.
- 2 Cliquez sur **Ajouter (+)**.
- 3 Sélectionnez **Orchestrator > Bibliothèque > Services Web Amazon > Elastic Cloud > Instances** et sélectionnez le workflow **Démarrer des instances** dans le dossier de workflows.
- 4 Cliquez sur **Suivant**.
- 5 Sélectionnez **Instance EC2** dans le menu déroulant **Type de ressource**.
Il s'agit du nom de la ressource correspondant à la ressource créée précédemment.
- 6 Sélectionnez **Instance** dans le menu déroulant **Paramètre d'entrée**.
Il s'agit du paramètre d'entrée du workflow d'actions sur les ressources devant correspondre au mappage de ressources.
- 7 Cliquez sur **Suivant**.
- 8 Laissez le nom et la description tels qu'ils s'affichent.
Le nom par défaut de l'action sur les ressources est Démarrer des instances.
- 9 Cliquez sur **Suivant**.
- 10 Laissez les champs tels qu'ils s'affichent dans l'onglet **Formulaire**.
- 11 Cliquez sur **Ajouter**.

Vous avez créé une action sur les ressources pour démarrer des machines virtuelles Amazon et vous pouvez la voir apparaître sur la page Actions sur les ressources.

Suivant

[Publier l'action pour le démarrage des instances d'Amazon.](#)

Publier l'action pour le démarrage des instances d'Amazon

Pour utiliser l'action sur la ressource Démarrer des instances créée récemment pour le des opérations de post-provisionnement sur des machines virtuelles Amazon, vous devez la publier.

Prérequis

Connectez-vous à la console vRealize Automation en tant qu'**architecte XaaS**.

Procédure

- 1 Sélectionnez **Conception > XaaS > Actions sur les ressources**.
- 2 Sélectionnez la ligne de l'action sur la ressource Démarrer des instances et cliquez sur **Publier**.

L'état de l'action sur la ressource Démarrer des instances passe à Publiée.

Suivant

Ajoutez l'action Démarrer des instances au droit d'accès qui inclut l'élément du catalogue Amazon. Reportez-vous à [Autoriser des utilisateurs à accéder à des services, des éléments de catalogue et des actions](#).

Dépannage d'accents et de caractères spéciaux incorrects dans les Blueprints XaaS

Lorsque vous créez des Blueprints XaaS dans des langues qui utilisent des chaînes non ASCII, les accents et les caractères spéciaux s'affichent dans un format inutilisable.

Cause

Vous pouvez activer une propriété de configuration de vRealize Orchestrator désactivée par défaut.

Solution

- 1 Sur le système du serveur Orchestrator, accédez à `/etc/vco/app-server/`.
- 2 Ouvrez le fichier de configuration `vmo.properties` dans un éditeur de texte.
- 3 Vérifiez que la propriété suivante est désactivée.

```
com.vmware.o11n.webview.htmlescaping.disabled
```

- 4 Enregistrez le fichier `vmo.properties`.
- 5 Redémarrez le serveur vRealize Orchestrator.

Publication d'un Blueprint

Les Blueprints sont enregistrés à l'état de brouillon et doivent être publiés manuellement avant que vous puissiez les configurer comme éléments du catalogue ou les utiliser comme composants de Blueprint dans le canevas de conception.

Après avoir publié le Blueprint, vous pouvez l'autoriser afin de le rendre disponible pour les demandes de provisionnement dans le catalogue de services.

Vous avez besoin de publier un Blueprint une fois seulement. Toute modification apportée à un Blueprint publié sont automatiquement reflétées dans le catalogue et dans les composants du blueprint imbriqué.

Publier un Blueprint

Vous pouvez publier un Blueprint à utiliser lors du provisionnement d'une machine et à réutiliser (en option) dans un autre Blueprint. Pour utiliser le Blueprint pour demander le provisionnement d'une machine, vous devez autoriser le Blueprint après l'avoir publié. Les Blueprints consommés comme des composants d'autres Blueprints n'ont pas besoin de droits d'accès.

Prérequis

- Connectez-vous à la console vRealize Automation en tant qu'**architecte d'infrastructure**.
- Créez un Blueprint. Consultez la *Liste de contrôle pour la création de Blueprints vRealize Automation*.

Procédure

- 1 Cliquez sur l'onglet **Conception**.
- 2 Cliquez sur **Blueprints**.
- 3 Pointez vers le Blueprint à publier et cliquez sur **Publier**.
- 4 Cliquez sur **OK**.

Le Blueprint est publié comme un élément du catalogue mais vous devez d'abord l'autoriser pour le rendre disponible pour les utilisateurs dans le catalogue de services.

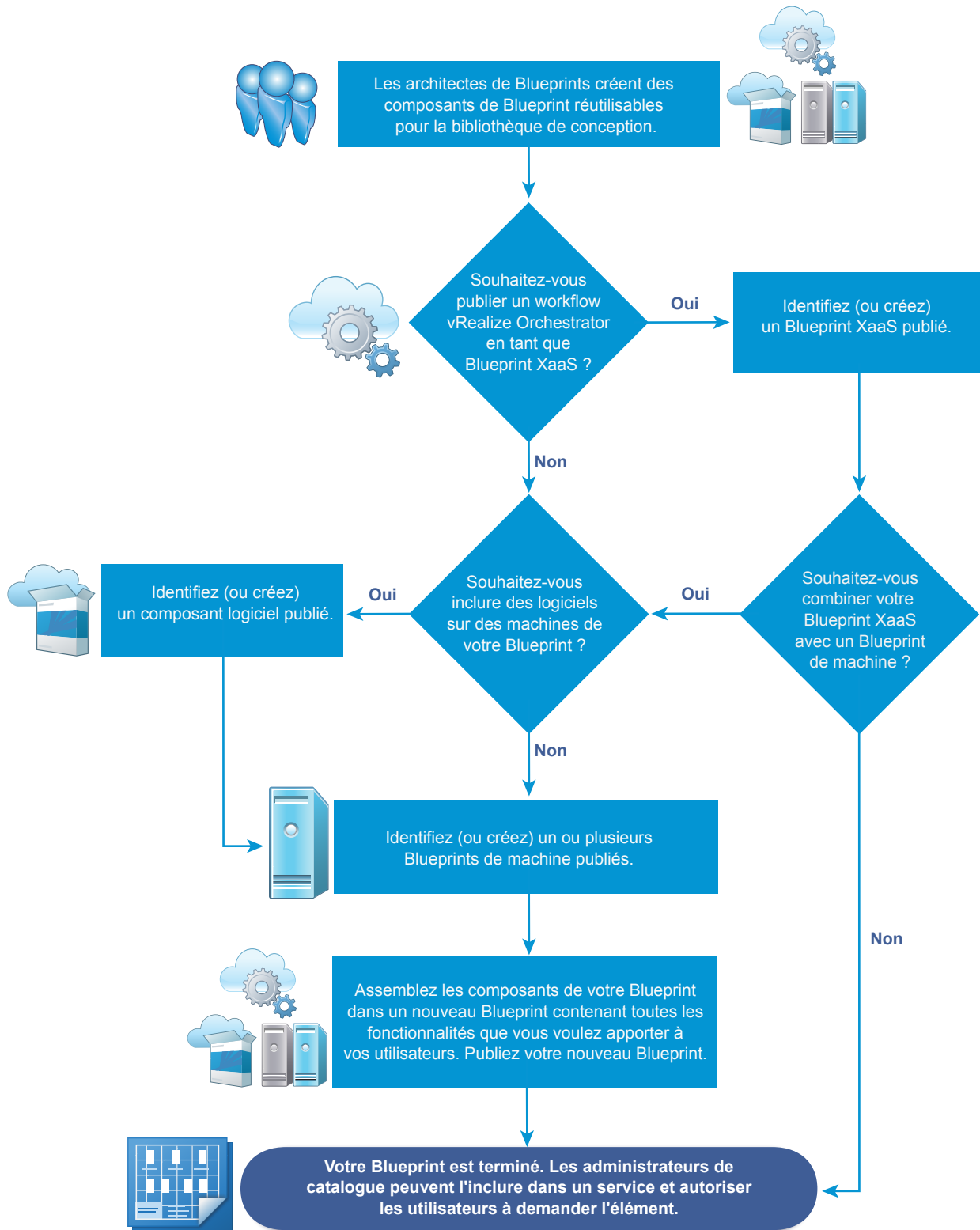
Suivant

Ajoutez le Blueprint au service du catalogue et autorisez les utilisateurs à demander l'élément du catalogue pour le provisionnement de machine défini dans le Blueprint.

Assemblage de Blueprints composites

Vous pouvez réutiliser des Blueprints publiés et des composants de Blueprint en les combinant d'une nouvelle façon afin de créer des modules de services informatiques qui offrent une fonctionnalité élaborée aux utilisateurs.

Figure 3-5. Workflow d'assemblage de Blueprints composites



- **Description du comportement d'un Blueprint imbriqué**

Vous pouvez réutiliser des Blueprints en les imbriquant dans un autre Blueprint en tant que composants. Vous imbriquez des Blueprints à des fins de réutilisation et de contrôle de modularité lors du provisionnement de machines. Dans ce cas, des règles et considérations spécifiques s'appliquent.

- **Sélection d'un composant de machine qui prend en charge des composants Logiciel**

Vous fournissez des composants Logiciel en les plaçant sur des composants de machine pris en charge lors de l'assemblage de Blueprints.

- **Création de liaisons de propriétés entre des composants de Blueprint**

Dans plusieurs scénarios de déploiement, un composant a besoin de la valeur de propriété d'un autre composant pour se personnaliser. Vous pouvez lier des propriétés de XaaS, de machines, de Logiciel et des propriétés personnalisées à d'autres propriétés dans un Blueprint.

- **Création de dépendances explicites et contrôle de l'ordre de provisionnement**

Si vous devez utiliser les informations d'un de vos composants de Blueprint pour compléter le provisionnement d'un autre composant, vous pouvez dessiner une dépendance explicite sur le canevas de conception pour échelonner le provisionnement afin que le composant dépendant ne soit pas provisionné de manière prématurée. Les dépendances explicites contrôlent l'ordre de construction d'un déploiement et déclenchent systématiquement des mises à jour dépendantes lors d'une opération de réduction de charge ou de montée en charge.

Description du comportement d'un Blueprint imbriqué

Vous pouvez réutiliser des Blueprints en les imbriquant dans un autre Blueprint en tant que composants. Vous imbriquez des Blueprints à des fins de réutilisation et de contrôle de modularité lors du provisionnement de machines. Dans ce cas, des règles et considérations spécifiques s'appliquent.

Un Blueprint qui contient un ou plusieurs Blueprints imbriqués est appelé Blueprint externe. Lorsque vous ajoutez un composant de Blueprint au canevas de conception en créant ou en modifiant un autre Blueprint, le composant du Blueprint est appelé Blueprint imbriqué et le Blueprint conteneur auquel il est ajouté est appelé Blueprint externe.

L'utilisation de Blueprints imbriqués implique des considérations qui ne sont pas toujours évidentes. Il est important de comprendre les règles et considérations suivantes afin de faire le meilleur usage possible de vos capacités de provisionnement de machines :

Règles et considérations générales relatives aux Blueprints imbriqués

- Il est recommandé de minimiser la complexité des Blueprints et de limiter les Blueprints à trois niveaux, avec le Blueprint de niveau supérieur utilisé à l'un de ces trois niveaux.
- Si un utilisateur a accès à un Blueprint externe, il a accès à ses Blueprints imbriqués.

- Vous pouvez appliquer une stratégie d'approbation à un Blueprint. Une fois approuvés, l'élément du catalogue de Blueprint et tous ses composants, y compris les Blueprints imbriqués, sont provisionnés. Vous pouvez également appliquer différentes stratégies d'approbation à différents composants. Toutes les stratégies d'approbation doivent être approuvées avant que le Blueprint requis ne soit provisionné.
- Lorsque vous modifiez un Blueprint publié, vous ne modifiez pas les déploiements déjà provisionnés à l'aide de ce Blueprint. Au moment du provisionnement, le déploiement résultant lit les valeurs actuelles depuis le Blueprint, y compris depuis les Blueprints imbriqués. Les seules modifications que vous pouvez appliquer aux déploiements provisionnés sont les modifications apportées aux composants logiciels, par exemple pour mettre à jour ou désinstaller des scripts.
- Les paramètres que vous définissez dans le Blueprint externe remplacent les paramètres configurés dans vos Blueprints imbriqués, à quelques exceptions près :
 - Vous pouvez modifier le nom d'un Blueprint imbriqué, mais vous ne pouvez pas modifier le nom d'un composant de machine ou de tout autre composant dans un Blueprint imbriqué.
 - Vous ne pouvez pas ajouter ou supprimer des propriétés personnalisées pour un composant de machine dans un Blueprint imbriqué. Vous pouvez toutefois modifier ces propriétés personnalisées. Vous ne pouvez pas ajouter, modifier ni supprimer des groupes de propriétés pour un composant de machine dans un Blueprint imbriqué.
- Les modifications que vous-même ou un autre architecte apportez aux paramètres des Blueprints imbriqués apparaissent dans les Blueprints externes, sauf si vous avez remplacés ces paramètres dans le Blueprint externe.
- Limitez la durée de bail maximale sur le Blueprint externe à la valeur de bail maximale la moins élevée d'un Blueprint de composant.

Bien que la durée de bail spécifiée sur un Blueprint imbriqué et sur le Blueprint externe peut être définie sur n'importe quelle valeur, la durée de bail maximale sur le Blueprint externe doit être limitée à la valeur de bail maximale la plus faible d'un Blueprint imbriqué. Cela permet à l'architecte d'application de concevoir un Blueprint composite ayant des valeurs de bail uniformes et variables tout en restant dans les limites définies par l'architecte d'infrastructure. Si la valeur de bail maximale définie sur un Blueprint imbriqué est inférieure à celle définie sur le Blueprint externe, la demande de provisionnement échoue.

- Lorsque vous utilisez un Blueprint externe, vous pouvez remplacer les paramètres Ressources de machine qui sont configurés pour un composant de machine dans un Blueprint imbriqué.
- Lorsque vous utilisez un Blueprint externe, vous pouvez glisser un composant logiciel vers un composant de machine d'un Blueprint imbriqué.
- Si vous ouvrez un Blueprint dans lequel un composant de machine dans un Blueprint imbriqué a été supprimé ou dont l'identifiant a été modifié, et si le composant de machine était associé à des composants dans le Blueprint actuel, les composants associés sont supprimés et le message suivant ou un message similaire s'affiche :

Un composant de machine dans un Blueprint imbriqué qui est référencé par des composants dans le Blueprint actuel a été supprimé ou son identifiant de composant de machine a été modifié. Tous les composants dans le Blueprint actuel qui étaient associés à l'identifiant de composant de machine manquant ou modifié ont été supprimés. Cliquez sur Annuler pour conserver l'historique de l'association entre l'identifiant de composant de machine manquant ou modifié dans le Blueprint imbriqué et les composants dans le Blueprint actuel et corrigez le problème dans le Blueprint imbriqué. Ouvrez le Blueprint imbriqué et ajoutez à nouveau le composant de machine manquant avec l'identifiant d'origine ou rétablissez l'identifiant d'origine du composant de machine. Cliquez sur Enregistrer pour supprimer tout l'historique de l'association entre l'identifiant de composant de machine manquant ou modifié dans le Blueprint imbriqué et les composants dans le Blueprint actuel.

Règles et considérations de réseau et de sécurité relatives aux Blueprints imbriqués

- Les composants réseau et de sécurité des Blueprints externes peuvent être associés à des machines qui sont définis dans des Blueprints imbriqués.
- Les composants réseau, de sécurité et d'équilibrage de charge NSX et leurs paramètres ne sont pas pris en charge dans les Blueprints imbriqués.
- Lorsque l'isolation d'application est appliquée dans le Blueprint externe, elle remplace les paramètres d'isolation d'application spécifiés dans les Blueprints imbriqués.
- Les paramètres de zone de transport qui sont définis dans le Blueprint externe remplacent les paramètres de zone de transport qui sont spécifiés dans les Blueprints imbriqués.
- Lorsque vous utilisez un Blueprint externe, vous pouvez définir les paramètres de l'équilibrage de charge relatifs aux paramètres des composants réseau et aux paramètres des composants de machine qui sont configurés dans un Blueprint interne ou imbriqué.
- Pour un Blueprint imbriqué qui contient un composant réseau NAT à la demande, la plage d'adresses IP spécifiée sur ce composant réseau NAT à la demande n'est pas modifiable dans le Blueprint externe.
- Le Blueprint externe ne peut pas contenir de Blueprint interne contenant des paramètres réseau ou des paramètres d'équilibrage de charge à la demande. L'utilisation d'un Blueprint interne contenant un composant réseau NSX ou un composant d'équilibrage de charge NSX n'est pas prise en charge.
- Pour un Blueprint imbriqué qui contient des composants réseau ou de sécurité NSX, vous ne pouvez pas modifier le profil réseau ou les informations relatives aux stratégies de sécurité spécifiées dans le Blueprint imbriqué. Toutefois, vous pouvez réutiliser ces paramètres pour d'autres composants de machine vSphere que vous ajoutez au Blueprint externe.
- Afin de s'assurer que les composants réseau et de sécurité NSX des Blueprints imbriqués disposent d'un nom unique dans un Blueprint composite, vRealize Automation préfixe les noms des composants réseau et de sécurité qui ne sont pas uniques avec l'identifiant du Blueprint imbriqué. Par exemple, si vous ajoutez un Blueprint ayant pour identifiant xbp_1 à un autre Blueprint et que les

deux Blueprints contiennent un composant de groupe de sécurité à la demande nommé `OD_Security_Group_1`, le composant du Blueprint imbriqué est renommé `xbp_1_OD_Security_Group_1` dans le canevas de conception du Blueprint. Les noms des composants réseau et de sécurité dans le Blueprint externe ne sont pas préfixés.

- Les paramètres de composant varient selon les Blueprints sur lesquels se trouve le composant. Par exemple, si vous ajoutez des groupes de sécurité, des balises de sécurité ou des réseaux à la demande aux niveaux de Blueprint interne et externe, les paramètres du Blueprint externe remplacent ceux du Blueprint interne. Les composants réseau et sécurité sont uniquement pris en charge au niveau du Blueprint externe à l'exception des réseaux existants qui fonctionnent au niveau du Blueprint interne. Pour éviter ces problèmes, ajoutez tous vos groupes de sécurité, balises de sécurité et réseaux à la demande uniquement au Blueprint externe.

Considérations relatives aux composants logiciels pour l'imbrication de Blueprints

Pour les Blueprints évolutifs, il est recommandé de créer des Blueprints d'une seule couche qui ne réutilisent pas d'autres Blueprints. En règle générale, les processus de mise à jour lors des opérations de dimensionnement sont déclenchés par des dépendances implicites, telles que les dépendances que vous créez lorsque vous liez une propriété logicielle à la propriété d'une machine. Cependant, les dépendances implicites contenues dans un Blueprint imbriqué ne déclenchent pas toujours de processus de mise à jour. Si vous devez utiliser des Blueprints imbriqués dans un Blueprint évolutif, vous pouvez dessiner manuellement des dépendances entre les composants contenus dans votre Blueprint imbriqué afin de créer des dépendances explicites qui déclenchent systématiquement une mise à jour.

Sélection d'un composant de machine qui prend en charge des composants Logiciel

Vous fournissez des composants Logiciel en les plaçant sur des composants de machine pris en charge lors de l'assemblage de Blueprints.

Pour prendre en charge les composants Logiciel, le Blueprint de machine sélectionné doit contenir un composant de machine basé sur un modèle, un snapshot ou une image de machine Amazon qui contient l'agent invité et l'agent de démarrage Logiciel. Ce Blueprint doit aussi utiliser une méthode de provisionnement prise en charge.

Étant donné que les agents Logiciel ne prennent pas en charge le protocole Internet version 6 (IPv6), utilisez les paramètres IPv4.

Si vous concevez des Blueprints évolutifs, il est recommandé de créer des Blueprints d'une seule couche qui ne réutilisent pas d'autres Blueprints. Normalement, les processus de mise à jour utilisés au cours des opérations de dimensionnement sont déclenchés par des dépendances implicites, telles que des liaisons de propriétés. Cependant, les dépendances implicites contenues dans un Blueprint imbriqué ne déclenchent pas toujours de processus de mise à jour.

Les architectes IaaS, les architectes d'application et les architectes de logiciel peuvent assembler des Blueprints. En revanche, seuls les architectes IaaS peuvent configurer des composants de machine. Si vous n'êtes pas un architecte IaaS, vous ne pouvez pas configurer vos propres composants de machine. Toutefois, vous pouvez réutiliser des Blueprints de machine créés et publiés par l'architecte IaaS.

Pour ajouter des composants logiciels avec succès au canevas de conception, vous devez également disposer des rôles de membre du groupe d'activité, d'administrateur de groupe d'activité ou d'administrateur de locataire afin d'accéder au catalogue cible.

Si vous devez utiliser des Blueprints imbriqués dans un Blueprint évolutif, vous pouvez dessiner manuellement des dépendances entre les composants contenus dans votre Blueprint imbriqué afin de créer des dépendances explicites qui déclenchent systématiquement une mise à jour.

Tableau 3-64. Méthodes de provisionnement prenant en charge Logiciel

Type de machine	Méthode de provisionnement
vSphere	Cloner
vSphere	Clone lié
vCloud Director	Cloner
vCloud Air	Cloner
Amazon AWS	Image de la machine Amazon

Création de liaisons de propriétés entre des composants de Blueprint

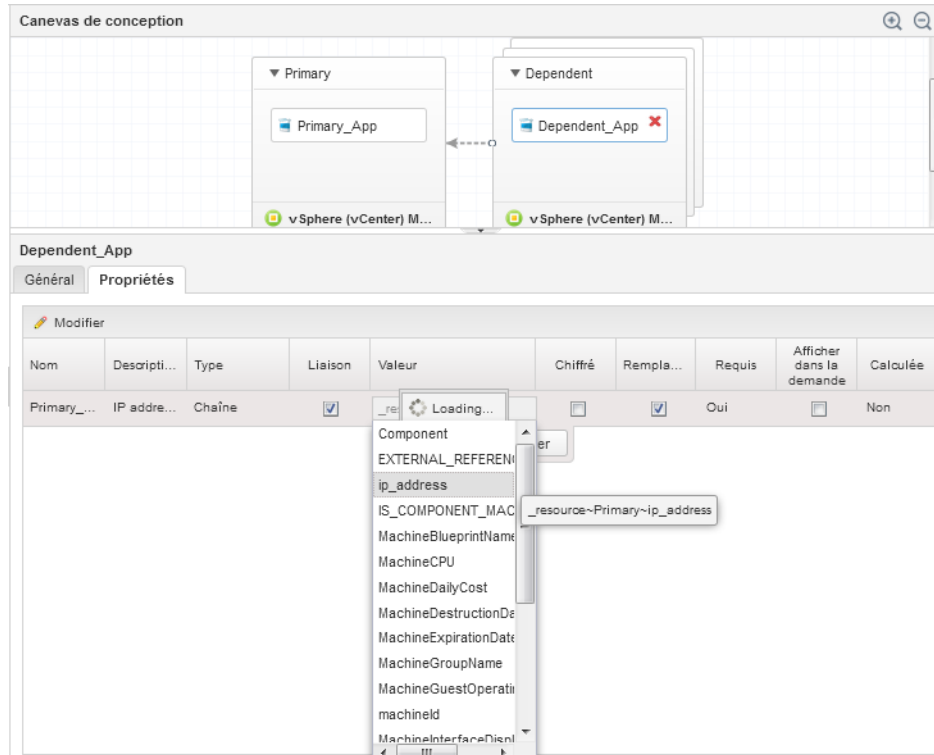
Dans plusieurs scénarios de déploiement, un composant a besoin de la valeur de propriété d'un autre composant pour se personnaliser. Vous pouvez lier des propriétés de XaaS, de machines, de Logiciel et des propriétés personnalisées à d'autres propriétés dans un Blueprint.

Par exemple, l'architecte de logiciel peut modifier des définitions de propriétés dans les scripts de cycle de vie d'un composant WAR. Un composant WAR peut avoir besoin de l'emplacement d'installation du composant du serveur Apache Tomcat. Par conséquent, l'architecte de logiciel doit configurer ce composant en définissant la valeur de la propriété `server_home` sur celle du serveur Apache Tomcat `install_path`. En tant qu'architecte de l'assemblage du Blueprint, vous devez lier la propriété `server_home` à la propriété `install_path` du serveur Apache Tomcat afin d'assurer le provisionnement correct du composant Logiciel.

Définissez les liaisons de propriétés lorsque vous configurez des composants dans un Blueprint. Sur la page du Blueprint, faites glisser le composant vers le canevas, puis cliquez sur l'onglet **Propriétés**. Pour lier une propriété à une autre dans un Blueprint, cochez la case **Lier**. Dans la zone de texte, entrez *ComponentName~PropertyName*. Autrement, utilisez la flèche Bas pour générer la liste des options de liaison disponibles. Pour délimiter les composants et les propriétés, utilisez le caractère du tilde ~. Par exemple, pour lier la propriété `dp_port`, vous pouvez taper `mysql~db_port` sur le composant logiciel.

MySQL. Pour lier des propriétés configurées lors du provisionnement, telles que l'adresse IP d'une machine ou le nom d'hôte d'un composant Logiciel, entrez `_resource~ComponentName~PropertyName`. Par exemple, pour lier le nom de réservation d'une machine, vous pouvez entrer `_resource~vSphere_Machine_1~MachineReservationName`.

Figure 3-6. Lier une propriété logicielle à l'adresse IP d'une machine



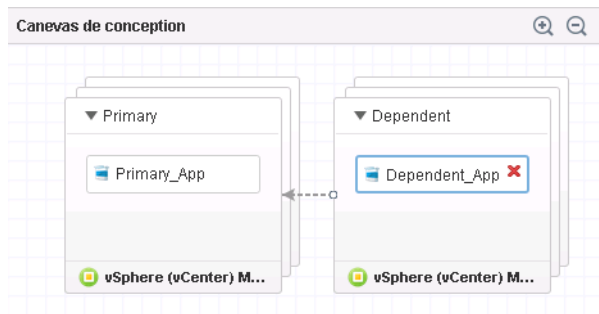
Création de dépendances explicites et contrôle de l'ordre de provisionnement

Si vous devez utiliser les informations d'un de vos composants de Blueprint pour compléter le provisionnement d'un autre composant, vous pouvez dessiner une dépendance explicite sur le canevas de conception pour échelonner le provisionnement afin que le composant dépendant ne soit pas provisionné de manière prématuré. Les dépendances explicites contrôlent l'ordre de construction d'un déploiement et déclenchent systématiquement des mises à jour dépendantes lors d'une opération de réduction de charge ou de montée en charge.

Lorsque vous concevez des Blueprints avec plusieurs machines et applications, certaines propriétés d'une machine peuvent être requises pour terminer l'installation d'une application sur une autre. Par exemple, si vous construisez un serveur Web, vous aurez éventuellement besoin du nom d'hôte du serveur de base de données pour pouvoir installer l'application et instancier les tables de base de données. Si vous mappez une dépendance explicite, votre serveur de base de données lance le provisionnement une fois que votre serveur Web l'a terminé.

Pour mapper une dépendance sur votre canevas de conception, dessinez une ligne allant du composant dépendant au composant dont vous dépendez. Lorsque vous avez terminé, le composant que vous souhaitez construire en deuxième étape comporte une flèche pointant vers le composant que vous souhaitez construire en premier. Par exemple, dans la figure Contrôle de l'ordre de construction en mappant les dépendances, la machine dépendante n'est provisionnée qu'une fois la machine principale construite. Vous pouvez également configurer le provisionnement simultané des deux machines mais dessiner une dépendance entre les composants logiciels.

Figure 3-7. Contrôle de l'ordre de construction en mappant les dépendances

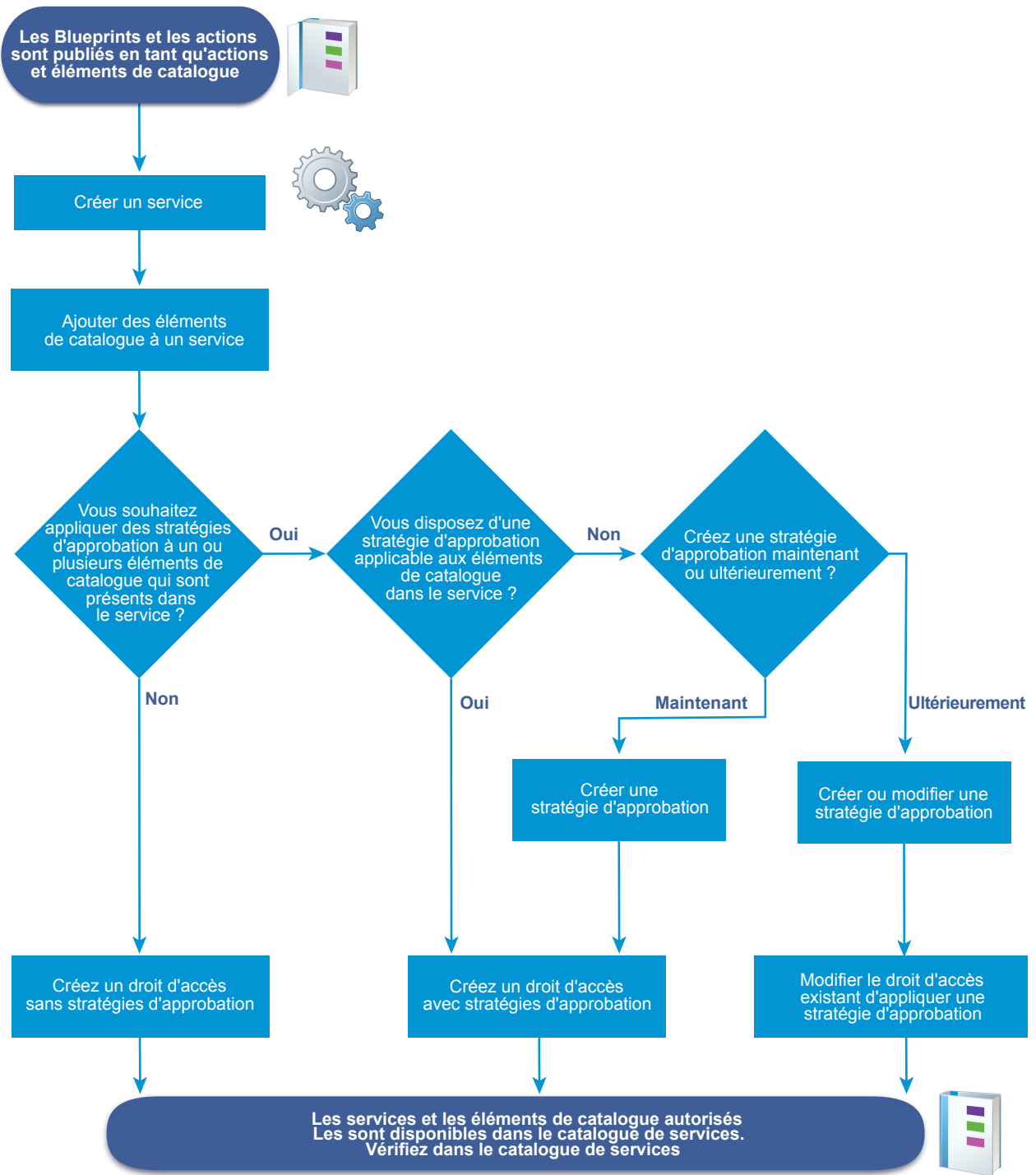


Si vous concevez des Blueprints évolutifs, il est recommandé de créer des Blueprints d'une seule couche qui ne réutilisent pas d'autres Blueprints. En règle générale, les processus de mise à jour lors des opérations de dimensionnement sont déclenchés par des dépendances implicites, telles que les dépendances que vous créez lorsque vous liez une propriété logicielle à la propriété d'une machine. Cependant, les dépendances implicites contenues dans un Blueprint imbriqué ne déclenchent pas toujours de processus de mise à jour. Si vous devez utiliser des Blueprints imbriqués dans un Blueprint évolutif, vous pouvez dessiner manuellement des dépendances entre les composants contenus dans votre Blueprint imbriqué afin de créer des dépendances explicites qui déclenchent systématiquement une mise à jour.

Gestion du catalogue de services

Le catalogue de services permet à vos clients de demander des machines et d'autres éléments à provisionner pour leur utilisation. Vous gérez l'accès utilisateur aux éléments du catalogue de services selon la manière dont vous construisez les services, autorisez les utilisateurs à accéder à un ou plusieurs éléments et appliquez le contrôle.

Le workflow que vous suivez pour ajouter des éléments au catalogue de services varie selon que vous créez et appliquez des stratégies d'approbation.



Liste de contrôle pour la configuration du catalogue de services

Après avoir créé et publié des Blueprints et des actions, vous pouvez créer un service vRealize Automation, configurer des éléments du catalogue et attribuer des droits d'accès ainsi que des approbations.

La liste de contrôle de la configuration du catalogue de services fournit une présentation de haut niveau des étapes requises pour configurer le catalogue. Elle propose également des liens vers des points de décision ou des instructions détaillées pour chaque étape.

Tableau 3-65. Liste de contrôle de la configuration du catalogue de services

Tâche	Rôle requis	Détails
<input type="checkbox"/> Ajouter un service	Administrateur de locataire ou administrateur du catalogue	Reportez-vous à Ajouter un service .
<input type="checkbox"/> Ajouter un élément du catalogue à un service	Administrateur de locataire ou administrateur du catalogue	Reportez-vous à Ajouter des éléments de catalogue à un service .
<input type="checkbox"/> Configurer l'élément du catalogue dans le service	Administrateur de locataire ou administrateur du catalogue	Reportez-vous à Configurer un élément du catalogue .
<input type="checkbox"/> Créer et appliquer des droits d'accès à un élément du catalogue	Administrateur de locataire ou gestionnaire de groupes d'activité	Reportez-vous à Autoriser des utilisateurs à accéder à des services, des éléments de catalogue et des actions .
<input type="checkbox"/> Créer et appliquer des stratégies d'approbation à un élément du catalogue	L'administrateur de locataire ou l'administrateur d'approbations peuvent créer des stratégies d'approbation. L'administrateur de locataire ou le gestionnaire de groupes d'activité peuvent appliquer des stratégies d'approbation.	Reportez-vous à Créer une stratégie d'approbation .

Création d'un service

Un service est un groupe d'éléments de catalogue que vous souhaitez que le catalogue de services comprenne. Vous pouvez autoriser le service, ce qui autorise les utilisateurs de groupe d'activité à accéder à tous les éléments du catalogue associé, et vous pouvez appliquer une stratégie d'approbation au service.

Un service fonctionne comme un groupe dynamique d'éléments de catalogue. Si vous autorisez un service, tous les éléments du catalogue associé au service sont disponibles dans le catalogue de services pour les utilisateurs spécifiés, et tous les éléments de catalogue que vous ajoutez ou supprimez d'un service affectent le catalogue de services.

Lorsque vous créez le service, vous pouvez l'utiliser comme catégorie de services de manière à réunir des offres de service pour les utilisateurs de votre catalogue de services. Par exemple, un service de bureau Windows qui inclut les éléments du catalogue de systèmes d'exploitation Windows 7, 8 et 10 ou un service Linux qui inclut les éléments de système d'exploitation CentOS et RHEL.

Ajouter un service

Vous pouvez ajouter un service afin de mettre les éléments du catalogue à disposition des utilisateurs du catalogue de services. Tous les éléments du catalogue doivent être associés à un service de façon à pouvoir autoriser les utilisateurs à accéder à ces éléments.

Lorsque les utilisateurs sont autorisés à accéder au service, les éléments apparaissent tous dans le catalogue de services. Vous pouvez également autoriser les utilisateurs à accéder à chaque élément du catalogue.

Prérequis

Connectez-vous à la console vRealize Automation en tant qu'**administrateur de locataire** ou **administrateur de catalogue**.

Procédure

1 Sélectionnez **Administration > Gestion de catalogue > Services**.

2 Cliquez sur l'icône **Nouveau (+)**.

3 Entrez un nom et une description.

Ces valeurs apparaissent dans le catalogue du service pour les utilisateurs du catalogue.

4 Pour ajouter une icône spécifique à un service dans le catalogue de services, cliquez sur **Parcourir** et sélectionnez une image.

Les types de fichiers image pris en charge sont GIF, JPG et PNG. Le format de l'image affichée est 40 x 40 pixels. Si vous ne sélectionnez pas une image personnalisée, l'icône par défaut apparaît dans le catalogue de services.

5 Sélectionnez un statut dans le menu déroulant **Statut**.

Option	Description
Inactif	Le service n'est pas disponible dans le catalogue de services. Lorsqu'un service est dans cet état, vous pouvez associer des éléments du catalogue au service, mais vous ne pouvez pas autoriser les utilisateurs à accéder à ce service. Si vous sélectionnez l'état Inactif pour un service actif autorisé, ce service est supprimé du catalogue de services jusqu'à ce que vous le réactiviez.
Actif	(Par défaut) Le service et les éléments du catalogue associés peuvent être mis à disposition des utilisateurs disposant d'une autorisation d'accès, dans le catalogue de services.
Supprimé	Supprime le service de vRealize Automation. Tous les éléments du catalogue associés demeurent, mais plus aucun élément associé au service n'est disponible dans le catalogue de services pour les utilisateurs.

6 Configurez les paramètres du service.

Les paramètres suivants fournissent des informations aux utilisateurs du catalogue de services. Ces paramètres n'affectent pas la disponibilité du service.

Option	Description
Heures	Configurez l'heure qui coïncide avec la disponibilité de l'équipe du support. L'heure est basée sur l'heure locale. Les heures de service ne peuvent pas s'étendre sur 2 jours consécutifs. Par exemple, vous ne pouvez pas définir les heures de service couvrant la période de 16h00 à 4h00. Pour aller au-delà de minuit, créez deux droits d'accès. Le premier droit couvre la période allant de 16 h 00 à 00 h 00, et le deuxième couvre la période allant de 00 h 00 à 04 h 00.
Propriétaire	Déterminez l'utilisateur ou le groupe d'utilisateur qui est le propriétaire principal du service et des éléments du catalogue associés.
Équipe de support	Déterminez le groupe d'utilisateur ou l'utilisateur personnalisé qui est disponible pour résoudre un problème que les utilisateurs du catalogue rencontrent lorsqu'ils provisionnent les éléments à l'aide de ce service.
Période de modification	Sélectionnez la date et l'heure auxquelles vous prévoyez de modifier le service. La date et l'heure spécifiées sont données à titre d'information et n'affectent pas la disponibilité du service.

7 Cliquez sur **Ajouter**.

Suivant

Associez les éléments du catalogue à un service de façon à pouvoir autoriser les utilisateurs à accéder à ces éléments. Reportez-vous à [Ajouter des éléments de catalogue à un service](#).

Ajouter des éléments de catalogue à un service

Ajouter des éléments de catalogue à des services de façon à pouvoir autoriser les utilisateurs à demander les éléments dans le catalogue de services. Un élément de catalogue peut être associé à un seul service.

Prérequis

- Connectez-vous à la console vRealize Automation en tant qu'**administrateur de locataire** ou **administrateur de catalogue**.
- Vérifier qu'un service existe. Reportez-vous à [Ajouter un service](#).
- Vérifiez qu'un ou plusieurs éléments de catalogues sont publiés. Reportez-vous à [Configurer un élément du catalogue](#).

Procédure

- 1 Sélectionnez **Administration > Gestion de catalogue > Services**.
- 2 Sélectionnez le service auquel vous ajoutez les éléments de catalogue, puis cliquez sur **Gérer les éléments du catalogue**.

3 Cliquez sur l'icône **Éléments du catalogue** (+).

- a Sélectionnez les éléments à inclure dans le service.

La boîte de dialogue Sélectionner les éléments du catalogue affiche uniquement les éléments qui ne sont pas associés à un service.

- b Cliquez sur **Ajouter**.

4 Cliquez sur **Fermer**.

Suivant

- Vous pouvez ajouter une icône personnalisée à l'élément du catalogue qui apparaîtra avec l'élément dans le catalogue de services. Reportez-vous à [Configurer un élément du catalogue](#).
- Autorisez les utilisateurs à accéder aux services ou aux éléments de catalogue de sorte qu'ils puissent les demander dans le catalogue de services. Reportez-vous à [Création de droits](#).

Utilisation d'éléments du catalogue et d'actions

Les éléments du catalogue sont des Blueprints publiés pour des machines, des composants logiciels ainsi que pour d'autres objets. Les actions de la gestion du catalogue sont des actions publiées, que vous pouvez exécuter sur les éléments du catalogue provisionnés. Vous pouvez utiliser les listes pour déterminer quels Blueprints et quelles actions sont publiés afin de les rendre disponibles pour les utilisateurs du catalogue de services.

Éléments du catalogue publiés

Un élément du catalogue est un Blueprint publié. Les Blueprints publiés peuvent également être utilisés dans d'autres Blueprints. La réutilisation de Blueprints dans d'autres Blueprints ne s'affiche pas dans la liste des éléments du catalogue.

Les éléments du catalogue publiés peuvent également inclure des éléments qui ne sont que des composants de Blueprints. Par exemple, des composants logiciels publiés sont répertoriés en tant qu'éléments du catalogue alors qu'ils ne sont disponibles que dans le cadre d'un déploiement.

Les éléments du catalogue de déploiement doivent être associés à un service afin que vous puissiez les rendre disponibles dans le catalogue de services pour les utilisateurs autorisés. Seuls les éléments actifs s'affichent dans le catalogue de services. Vous pouvez configurer des éléments du catalogue sur un service différent, les désactiver si vous souhaitez les supprimer temporairement du catalogue de services et ajouter une icône personnalisée s'affichant dans le catalogue.

Actions publiées

Les actions sont des modifications que vous pouvez apporter aux éléments du catalogue provisionnés. Par exemple, vous pouvez redémarrer une machine virtuelle.

Les actions peuvent inclure des actions intégrées ou des actions créées à l'aide de XaaS. Les actions intégrées sont ajoutées lorsque vous ajoutez une machine ou un autre Blueprint fourni. Les actions XaaS doivent être créées et publiées.

L'action n'est pas associée aux services. Vous devez l'inclure dans le droit d'accès qui contient l'élément du catalogue sur lequel l'action est exécutée. Les actions accordées aux utilisateurs ne s'affichent pas dans le catalogue de services. Les actions sont disponibles pour l'élément provisionné dans l'onglet **Éléments** de l'utilisateur du catalogue de services s'ils s'appliquent à l'élément et l'état actuel de celui-ci.

Vous pouvez ajouter une icône personnalisée à l'action s'affichant dans l'onglet **Éléments**.

Configurer un élément du catalogue

Un élément du catalogue est un Blueprint publié dont vous pouvez autoriser l'accès aux utilisateurs. Les options des éléments du catalogue permettent de changer l'état ou le service associés. Vous pouvez également afficher les droits qui incluent l'élément du catalogue sélectionné.

Seuls les éléments du catalogue associés à un service, et pour lesquels les utilisateurs possèdent un droit d'accès, apparaissent dans le catalogue de services. Il est possible d'associer un élément du catalogue à un seul service uniquement.

Si vous souhaitez qu'un élément du catalogue ne figure pas dans le catalogue des services sans devoir pour cela le retirer d'un droit ou de la liste des éléments du catalogue publiés, vous pouvez le désactiver. L'état d'un élément du catalogue désactivé est Retiré dans la grille et Inactif dans les détails de configuration. Vous pouvez le réactiver ultérieurement.

Prérequis

- Connectez-vous à la console vRealize Automation en tant qu'**administrateur de locataire** ou **administrateur de catalogue**.
- Vérifiez qu'au moins un Blueprint est publié en tant qu'élément du catalogue. Reportez-vous à [Publier un Blueprint](#).

Procédure

- 1 Sélectionnez **Administration > Gestion de catalogue > Éléments du catalogue**.
- 2 Sélectionnez l'élément du catalogue et cliquez sur **Configurer**.

3 Configurez les paramètres de l'élément du catalogue.

Option	Description
 Icône 	Accédez à une image. Les types de fichiers image pris en charge sont GIF, JPG et PNG. Le format de l'image affichée est 40 x 40 pixels. Si vous ne sélectionnez pas une image personnalisée, l'icône du catalogue par défaut apparaît dans le catalogue de services.
État	<p>Les valeurs possibles sont les suivantes : Actif, Inactif et Intermédiaire.</p> <ul style="list-style-type: none"> ■ Actif. L'élément du catalogue apparaît dans le catalogue de services et les utilisateurs autorisés peuvent s'en servir pour provisionner des ressources. Il figure dans la liste des éléments du catalogue avec l'état Publié. ■ Inactif. L'élément n'est pas disponible dans le catalogue de services. Il figure dans la liste des éléments du catalogue avec l'état Retiré. ■ Intermédiaire. L'élément n'est pas disponible dans le catalogue de services. Sélectionnez cette option de menu si l'élément a été inactif pour indiquer que vous envisagez de le réactiver. Il figure dans la liste des éléments du catalogue avec l'état Intermédiaire.
Service	Sélectionnez un service. Vous devez associer chaque élément du catalogue à un service si vous souhaitez que ce dernier figure dans le catalogue de services pour les utilisateurs autorisés. La liste inclut les services actifs et inactifs.
Nouveau et intéressant	L'élément du catalogue apparaît dans la zone Nouveau et intéressant de la page d'accueil.

4 Pour afficher les droits donnant aux utilisateurs accès à l'élément du catalogue, cliquez sur l'onglet **Droits**.

5 Cliquez sur **Mise à jour**.

Suivant

- Pour rendre l'élément disponible dans le catalogue de services, accordez aux utilisateurs le droit d'accès au service associé à l'élément ou à l'élément lui-même. Reportez-vous à [Création de droits](#).
- Pour spécifier l'ordre de traitement des droits d'accès afin que les stratégies d'approbation de chaque utilisateur soient correctement appliquées, définissez l'ordre de priorité de plusieurs droits d'accès pour le même groupe d'activité. Reportez-vous à [Définir l'ordre de priorité des droits d'accès](#).

Configurer une action pour le catalogue de services

Une action est une modification ou un workflow pouvant être exécuté sur des éléments provisionnés. Vous pouvez ajouter une icône ou afficher les droits d'accès qui incluent l'action sélectionnée.

Une action est soit une action intégrée pour une machine provisionnée, un réseau et d'autres composants du Blueprint, ou une action XaaS publiée.

Pour l'icône, les types de fichiers d'images pris en charge sont GIF, JPG et PNG. Le format de l'image affichée est 40 x 40 pixels. Si vous ne sélectionnez pas une image personnalisée, l'icône de l'action par défaut apparaît dans l'onglet **Éléments**.

Prérequis

- Connectez-vous à la console vRealize Automation en tant qu'**administrateur de locataire** ou **administrateur de catalogue**.
- Vérifiez que vous disposez d'au moins une action publiée. Reportez-vous à la section [Publier un Blueprint](#) et [Publier une action sur la ressource](#).

Procédure

- 1 Sélectionnez **Administration > Gestion de catalogue > Actions**.
- 2 Sélectionnez l'action partagée et cliquez sur **Afficher les détails**.
- 3 Accédez à une image.
- 4 Pour afficher les droits donnant accès à l'action aux utilisateurs, cliquez sur l'onglet **Droits**.
- 5 Cliquez sur **Mise à jour**.

Suivant

[Autoriser des utilisateurs à accéder à des services, des éléments de catalogue et des actions.](#)

Création de droits

Les droits contrôlent quels éléments et actions sont disponibles dans le catalogue de services pour les membres du groupe d'activité sélectionné. Un droit d'accès doit être actif pour que les éléments apparaissent dans le catalogue de services. Si vous avez des éléments qui nécessitent une gouvernance, vous pouvez utiliser des droits d'accès pour appliquer des stratégies d'approbation aux différents éléments.

Pour configurer le droit d'accès, les éléments du catalogue doivent être inclus dans un service. Les droits peuvent inclure plusieurs services, des éléments de catalogue de services qui sont inclus dans d'autres droits, ainsi que des actions que vous pouvez exécuter sur les éléments de catalogue déployés.

Comprendre les interactions des options de droit

Le mode de configuration d'un droit détermine ce qui figure dans le catalogue de services. L'interaction entre services, éléments du catalogue et composants, action et stratégies d'approbation a une incidence sur ce que l'utilisateur du catalogue de services peut demander et comment les stratégies d'approbation sont appliquées.

Lorsque vous créez un droit d'accès, vous devez prendre en compte les interactions des services, les éléments de catalogue, les actions et les approbations.

■ [Services dans les droits d'accès](#)

Un service autorisé fonctionne comme un groupe dynamique d'éléments de catalogue. Si un élément de catalogue est ajouté à un service après avoir été autorisé, le nouvel élément de catalogue est disponible pour les utilisateurs spécifiés sans configuration supplémentaire.

- **Éléments de catalogue et composants des droits**

Les éléments de catalogue sont des Blueprints que vous pouvez demander dans le catalogue de services. Les composants autorisés font partie des Blueprints, mais vous ne pouvez pas les demander spécifiquement dans le catalogue de services.

- **Action dans les droits**

Actions exécutées sur des éléments de catalogue déployés. Les éléments de catalogue provisionnés, et les actions que vous êtes autorisé à exécuter sur ceux-ci, s'affichent dans l'onglet Éléments. Pour exécuter des actions sur un élément déployé, l'action doit être incluse dans le même droit que l'élément de catalogue qui a provisionné l'élément à partir du catalogue de services.

- **Stratégies d'approbation des droits**

Les stratégies d'approbations sont appliquées aux droits afin que vous puissiez gérer des ressources de votre environnement.

Services dans les droits d'accès

Un service autorisé fonctionne comme un groupe dynamique d'éléments de catalogue. Si un élément de catalogue est ajouté à un service après avoir été autorisé, le nouvel élément de catalogue est disponible pour les utilisateurs spécifiés sans configuration supplémentaire.

Si vous appliquez une stratégie d'approbation à un service, tous les éléments, lorsqu'ils sont demandés, sont soumis à la même stratégie d'approbation.

Éléments de catalogue et composants des droits

Les éléments de catalogue sont des Blueprints que vous pouvez demander dans le catalogue de services. Les composants autorisés font partie des Blueprints, mais vous ne pouvez pas les demander spécifiquement dans le catalogue de services.

Les éléments du catalogue et les composants autorisés peuvent inclure les éléments suivants :

Éléments du catalogue

- Les éléments d'un service que vous souhaitez fournir à des utilisateurs autorisés, même les services non inclus dans le droit d'accès actuel.

Par exemple, en tant qu'administrateur du catalogue, vous avez associé plusieurs versions différentes de Red Hat Enterprise Linux à un service Red Hat et autorisé le service aux ingénieurs qualité pour le produit A. Vous recevez alors une demande de création d'éléments du catalogue de services incluant uniquement la dernière version des systèmes d'exploitation exécutés sous Linux pour l'équipe de formation. Vous créez un droit d'accès pour l'équipe de formation qui inclut les dernières versions des systèmes d'exploitation dans un service. La dernière version de RHEL est déjà associée à un autre service, et vous ajoutez donc RHEL comme élément de catalogue au lieu d'ajouter l'intégralité du service Red Hat.

- Des éléments inclus dans un service qui sont inclus dans le droit d'accès actuel, mais vous souhaitez appliquer une stratégie d'approbation à l'élément de catalogue individuel qui est différente de la stratégie que vous avez appliquée au service.

Par exemple, en tant que gestionnaire de groupes d'activité, vous autorisez l'équipe de développement à accéder à un service qui inclut trois éléments du catalogue de machines virtuelles. Vous appliquez une stratégie d'approbation qui exige l'approbation de l'administrateur de l'infrastructure virtuelle pour les machines avec plus de quatre CPU. Une des machines virtuelles étant utilisée pour les tests de performances, vous l'ajoutez donc en tant qu'élément du catalogue et vous appliquez une stratégie d'approbation moins restrictive à ce même groupe d'utilisateurs.

Composants

- Les composants ne sont pas disponibles par nom dans le catalogue de services, car ils font partie d'un élément de catalogue. Vous les autorisez individuellement afin de pouvoir appliquer une stratégie d'approbation spécifique qui diffère de celle de l'élément de catalogue dans lequel ils sont inclus.

Par exemple, un élément inclut une machine et des logiciels. La machine est disponible en tant qu'élément pouvant être provisionné et a une stratégie d'approbation qui exige l'approbation du responsable du site. Les logiciels ne sont pas disponibles en tant qu'éléments autonomes et pouvant être provisionnés, mais uniquement dans le cadre d'une demande de machine. En outre, la stratégie d'approbation des logiciels exige l'approbation de l'administrateur chargé des licences logicielles de l'organisation. Lorsque la machine est demandée dans le catalogue de services, elle doit être approuvée par l'administrateur du site et l'administrateur chargé d'octroyer les licences des logiciels avant d'être provisionnée. Une fois provisionnée, la machine (avec l'entrée logicielle correspondante) est affichée dans l'onglet Éléments du demandeur en tant que machine.

Action dans les droits

Actions exécutées sur des éléments de catalogue déployés. Les éléments de catalogue provisionnés, et les actions que vous êtes autorisé à exécuter sur ceux-ci, s'affichent dans l'onglet Éléments. Pour exécuter des actions sur un élément déployé, l'action doit être incluse dans le même droit que l'élément de catalogue qui a provisionné l'élément à partir du catalogue de services.

Par exemple, le droit d'accès 1 inclut une machine virtuelle vSphere et une action de création de snapshot, et le droit d'accès 2 inclut uniquement une machine virtuelle vSphere. Si vous déployez une machine vSphere avec le droit d'accès 1, l'action de création de snapshot est disponible. Si vous déployez une machine vSphere avec le droit d'accès 2, il n'y a pas d'action. Pour qu'une action soit disponible pour les utilisateurs avec le droit d'accès 2, ajoutez l'action de création de snapshot au droit d'accès 2.

Si vous sélectionnez une action qui ne s'applique à aucun des éléments du catalogue dans le droit d'accès, elle n'apparaîtra pas comme action dans l'onglet Éléments. Par exemple, votre droit d'accès inclut une machine vSphere et vous autorisez une action de destruction d'une machine dans le cloud. L'action de destruction n'est pas disponible pour être exécutée sur la machine provisionnée.

Vous pouvez appliquer une stratégie d'approbation à une action qui est différente de la stratégie appliquée à l'élément de catalogue dans le droit d'accès.

Si l'utilisateur du catalogue de services est membre de plusieurs groupes d'activité, et si un seul groupe est autorisé à mettre sous tension et hors tension et que l'autre est uniquement autorisé à détruire, cet utilisateur aura accès à ces trois actions pour la machine provisionnée applicable.

Recommandations pour autoriser des utilisateurs à accéder à des actions

Les Blueprints sont complexes et les actions d'autorisation à exécuter sur des Blueprints provisionnés peuvent donner lieu à des comportements inattendus. Utilisez les recommandations suivantes lorsque vous autorisez les utilisateurs de catalogue de services à exécuter des actions sur leurs éléments provisionnés.

- Lorsque vous autorisez des utilisateurs à utiliser l'action de destruction de machine, autorisez-les également à exécuter une destruction de déploiement. Un Blueprint provisionné est un déploiement. Un déploiement peut contenir une machine. Si un utilisateur du catalogue de services est autorisé à exécuter l'action de destruction de machine mais pas celle de destruction de déploiement, lorsque l'utilisateur exécute l'action de destruction de machine sur la dernière ou la seule machine d'un déploiement, un message s'affiche indiquant qu'il ne possède pas les autorisations nécessaires pour exécuter l'action. Donnez les droits d'accès aux deux actions permet de s'assurer que le déploiement est supprimé de votre environnement. Pour gérer le contrôle de l'action de destruction de déploiement, vous pouvez créer une stratégie de pré-approbation et l'appliquer à l'action. Cette stratégie autorise l'approbateur désigné à valider la demande de destruction de déploiement avant qu'elle ne s'exécute.
- Lorsque vous autorisez les utilisateurs du catalogue de services à utiliser Modifier le bail, Changer le propriétaire, Expirer, Reconfigurer et d'autres actions applicables aux machines et aux déploiements, autorisez-les à exécuter les deux actions.

Stratégies d'approbation des droits

Les stratégies d'approbations sont appliquées aux droits afin que vous puissiez gérer des ressources de votre environnement.

Pour appliquer une stratégie d'approbation lorsque vous créez le droit d'accès, la stratégie doit déjà exister. Si elle n'existe pas, vous pouvez créer le droit d'accès et le laisser à l'état d'ébauche ou inactif jusqu'à ce que vous ayez créé les stratégies d'approbation nécessaires pour les éléments de catalogue et les actions dans ce droit d'accès, puis appliquer les stratégies par la suite.

Vous n'avez pas à appliquer une stratégie d'approbation aux éléments ou actions. Si aucune stratégie d'approbation n'est appliquée, les éléments et les actions sont déployés lorsqu'ils sont demandés sans déclencher de demande d'approbation.

Autoriser des utilisateurs à accéder à des services, des éléments de catalogue et des actions

Lorsque vous ajoutez un service, un élément de catalogue ou une action à un droit d'accès, vous autorisez les utilisateurs identifiés dans le droit d'accès à demander les éléments du catalogue de services pouvant être provisionnés. Des actions sont associées aux éléments et apparaissent dans l'onglet **Éléments** de l'utilisateur qui fait la demande.

Il existe plusieurs rôles d'utilisateur ayant l'autorisation de créer des droits d'accès pour les groupes d'activité.

- Les administrateurs de locataire peuvent créer des droits pour n'importe quel groupe d'activité dans leur locataire.

- Les gestionnaires de groupes d'activité peuvent créer des droits pour les groupes qu'ils gèrent.
- Les administrateurs de catalogue peuvent créer des droits d'accès pour n'importe quel groupe d'activité dans leur locataire.

Lorsque vous créez un droit d'accès, vous devez sélectionner un groupe d'activité et les membres de celui-ci qui disposeront de ce droit.

Pour savoir comment créer un droit d'accès de façon à pouvoir utiliser les interactions des services, éléments de catalogue et actions avec des approbations, reportez-vous à [Création de droits](#).

Prérequis

- Connectez-vous à la console vRealize Automation en tant qu'**administrateur de locataire** ou **administrateur de catalogue**.
- Vérifiez que les éléments du catalogue auxquels vous autorisez des utilisateurs à accéder sont associés à un service. Reportez-vous à [Ajouter des éléments de catalogue à un service](#).
- Vérifiez que le groupe d'activité pour lequel vous définissez le droit d'accès existe et que les utilisateurs membres et les groupes d'utilisateurs sont définis. Reportez-vous à [Créer un groupe d'activité](#).
- Vérifiez que les stratégies d'approbation existent si vous prévoyez d'ajouter des approbations lorsque vous créez ce droit d'accès. Reportez-vous à [Créer une stratégie d'approbation](#). Si vous souhaitez autoriser des utilisateurs à accéder au catalogue de services sans approbations, vous pouvez modifier le droit d'accès par la suite pour ajouter des approbations.

Procédure

- 1 Sélectionnez **Administration > Gestion de catalogue > Droits d'accès**.
- 2 Cliquez sur l'icône **Nouveau** (+).
- 3 Configurez les options **Détails**.

Les détails déterminent comment le droit d'accès apparaît dans la liste des droits d'accès et quels utilisateurs ont accès aux éléments dans le catalogue de services.

Option	Description
Nom et description	Informations sur le droit d'accès qui apparaissent dans la liste des droits d'accès.
Date d'expiration	Définissez la date et l'heure auxquelles vous souhaitez que le droit d'accès devienne actif sur un site spécifique.
État	<p>Les valeurs possibles sont Actif, Inactif et Supprimé.</p> <ul style="list-style-type: none"> ■ Actif : les éléments sont disponibles dans le catalogue de services. Cette option est disponible lorsque vous ajoutez ou modifiez des droits. ■ Inactif : les éléments ne sont pas disponibles dans le catalogue de services. Le droit a été désactivé par la date d'expiration ou par un utilisateur. ■ Supprimé : supprime le droit.

Option	Description
Groupe d'activité	<p>Sélectionnez un groupe d'activité. Vous pouvez créer des droits d'accès pour un seul groupe d'activité et les utilisateurs autorisés doivent être membres du groupe d'activité.</p> <p>Si vous souhaitez rendre un droit disponible pour tous les utilisateurs, un groupe d'activité Tous les utilisateurs doit avoir été créé, ou vous devez créer des droits pour chaque groupe d'activité.</p> <p>Si vous êtes connecté en tant que gestionnaire de groupe d'activité, vous pouvez créer des droits d'accès uniquement pour votre groupe d'activité.</p>
Utilisateurs et groupes	<p>Sélectionnez Tous les utilisateurs et groupes pour autoriser tous les membre du groupe d'activité à accéder aux éléments de catalogue et aux actions. Vous pouvez également autoriser des utilisateurs individuels ou des groupes. Pour activer un droit d'accès, vous devez sélectionner au moins un utilisateur de groupe d'activité ou groupe.</p>

4 Cliquez sur **Suivant**.

5 Cliquez sur une icône **Nouveau (+)** pour autoriser les utilisateurs à accéder aux services, aux éléments du catalogue ou aux actions avec ce droit d'accès.

Vous pouvez créer un droit d'accès avec différentes combinaisons de services, éléments et actions.

Option	Description
Services autorisés	<p>Ajoutez un service lorsque vous voulez permettre à des utilisateurs autorisés d'accéder à tous les éléments du catalogue publiés associés au service.</p> <p>Un service autorisé est un droit d'accès dynamique. Si un élément est ajouté au service par la suite, il est ajouté au catalogue de services des utilisateurs autorisés. Les droits d'accès incluent les services et les éléments du catalogue individuels.</p>
Éléments de catalogue et composants autorisés	<p>Ajoutez des éléments individuels qui sont disponibles pour les utilisateurs autorisés.</p> <p>Les droits d'accès incluent les services et les éléments du catalogue individuels. Pour appliquer une autre stratégie d'approbation à un élément inclus dans le service, ajoutez-la en tant qu'élément du catalogue. La stratégie d'approbation sur un élément est prioritaire sur la stratégie d'approbation sur le service auquel il appartient lorsqu'ils sont dans le même droit. S'ils sont dans différents droits, l'ordre est basé sur la priorité définie.</p> <p>Les éléments du catalogue doivent être associés à un service pour être disponibles dans le catalogue de services. L'élément du catalogue peut être associé à n'importe quel service et non pas uniquement à un service du droit d'accès actuel.</p> <p>Les composants font partie d'un élément de catalogue mais ne sont pas disponibles par nom dans le catalogue de services. Par exemple, le logiciel MySQL est un composant d'un élément de catalogue de machine virtuelle CentOS. Les composants sont autorisés avec l'élément de catalogue. Si vous souhaitez appliquer une stratégie d'approbation qui est spécifique au logiciel, vous autorisez l'élément individuellement. Sinon, vous n'avez pas besoin d'autoriser un composant pour le déployer avec l'élément parent.</p>

Option	Description
Actions autorisées	<p>Ajoutez des actions si vous souhaitez autoriser les utilisateurs à exécuter des actions pour un élément provisionné.</p> <p>Les actions que souhaitez exécuter sur les éléments provisionnés à partir de ce droit doivent être incluses dans le même droit d'accès.</p> <p>Les actions autorisées n'apparaissent pas dans le catalogue de services. Elles apparaissent dans l'onglet Éléments d'un élément provisionné.</p>
Les actions s'appliquent uniquement aux éléments définis dans ce droit.	<p>Détermine si les actions autorisées sont autorisées pour tous les éléments applicables du catalogue de services ou seuls les éléments dans ce droit.</p> <p>Si cette option est sélectionnée, les actions sont autorisées pour les membres du groupe d'activité pour les éléments applicables dans ce droit. Cette méthode pour autoriser les actions vous permet de spécifier les actions pour les éléments spécifiques.</p> <p>Si cette option n'est pas sélectionnée, les actions sont autorisées pour les utilisateurs spécifiés dans le droit pour tous les éléments de catalogue applicables, que les éléments soient inclus ou non dans ce droit. Toutes les stratégies d'approbation appliquées sur ces actions sont également actives.</p>

- 6 Pour filtrer les éléments disponibles, utilisez les menus déroulants dans chaque section.
- 7 Cochez les cases pour inclure des éléments au droit d'accès.
- 8 Pour ajouter une stratégie d'approbation au service, à l'élément ou à l'action sélectionné(e), sélectionnez une stratégie d'approbation dans le menu déroulant **Appliquer cette stratégie aux éléments sélectionnés**.

Si vous appliquez une stratégie d'approbation à un service, tous les éléments du service auront la même stratégie d'approbation. Pour appliquer une autre stratégie à un élément, ajoutez ce dernier en tant qu'élément de catalogue et appliquez la stratégie appropriée.

- 9 Cliquez sur **OK**.

Le service, l'élément ou l'action est ajouté(e) au droit d'accès.

- 10 Cliquez sur **Terminer** pour enregistrer le droit d'accès.

Si l'état du droit d'accès est Actif, le service et les éléments sont ajoutés au catalogue de services.

Suivant

Vérifiez que les services et les éléments de catalogue autorisés s'affichent dans le catalogue de services pour les utilisateurs autorisés et que les éléments demandés provisionnent les objets cibles comme prévu. Vous pouvez demander l'élément pour le compte des utilisateurs sélectionnés.

Définir l'ordre de priorité des droits d'accès

Si plusieurs droits d'accès existent pour le même groupe d'activité, vous pouvez définir l'ordre de priorité de sorte que lorsqu'un utilisateur de catalogue de services fait une demande, les droits d'accès et la stratégie d'approbation associée sont traités dans l'ordre spécifié.

Si vous configurez une stratégie d'approbation pour un groupe d'utilisateurs et que souhaitez qu'une stratégie soit appliquée à un seul membre du groupe pour un ou plusieurs des services, des éléments du catalogue ou des actions, définissez l'ordre de priorité des droits d'accès du membre avant ceux du groupe. Lorsque le membre demande un élément du catalogue de services, la stratégie d'approbation est appliquée en fonction de l'ordre de priorité des droits d'accès du groupe d'activité. La première fois que le nom du membre est trouvé, dans le cadre d'un groupe d'utilisateurs personnalisé ou d'un utilisateur individuel, c'est la stratégie d'approbation en application.

Par exemple, vous créez deux droits d'accès pour le même élément du catalogue de manière à appliquer une stratégie d'approbation au groupe d'utilisateurs de la comptabilité et une autre stratégie d'approbation pour Chris, un membre de ce groupe.

Tableau 3-66. Exemple de droits d'accès

Droit d'accès 1	Droit d'accès 2
Groupe d'activité : Finances	Groupe d'activité : Finances
Utilisateurs et groupes : Groupe de Comptabilité	Utilisateurs et groupes : Chris
Élément du catalogue 1 : Stratégie A	Élément du catalogue 1 : Stratégie C

Chris demande l'élément du catalogue 1 dans le catalogue de services. En fonction de l'ordre de priorité des droits d'accès du groupe d'activité Finances, une stratégie différente est appliquée à la demande de Chris.


Tableau 3-67. Exemples de résultats

Configuration et résultat	Ordre de priorité	Ordre de priorité
Ordre de priorité	1 : Droit d'accès 1 2 : Droit d'accès 2	1 : Droit d'accès 2 2 : Droit d'accès 1
Stratégie appliquée	La Stratégie A est appliquée. Chris est membre du groupe d'utilisateurs Comptabilité. La recherche de Chris en tant qu'utilisateur autorisé s'arrête à Droit d'accès 1 et la stratégie d'approbation est appliquée.	La Stratégie C est appliquée. La recherche de Chris en tant qu'utilisateur autorisé s'arrête à Droit d'accès 2 et la stratégie d'approbation est appliquée.

Prérequis

Connectez-vous à la console vRealize Automation en tant qu'**administrateur de locataire** ou **administrateur de catalogue**.

Procédure

- 1 Sélectionnez **Administration > Gestion de catalogue > Droits d'accès**.
- 2 Cliquez sur l'icône **Définir l'ordre de priorité** ().
- 3 Sélectionnez un groupe d'activité dans la liste déroulante **Groupe d'activité**.

- 4 Faites glisser un droit d'accès vers un nouvel emplacement de la liste pour modifier son ordre de priorité.
- 5 Sélectionnez une méthode de mise à jour.

Option	Description
Mettre à jour	Enregistre vos modifications.
Mettre à jour et fermer	Enregistre vos modifications et ferme la fenêtre Définir l'ordre de priorité des droits d'accès .

Utilisation de stratégies d'approbation

Les stratégies d'approbation sont des éléments de gouvernance que vous ajoutez aux demandes de catalogue de services de manière à pouvoir gérer les ressources dans votre environnement. Chaque stratégie est constituée d'un ensemble de conditions qui peuvent être appliquées aux services, aux éléments de catalogue et aux actions lorsque vous autorisez des utilisateurs à accéder à ces éléments.

Procédure de stratégie d'approbation

En premier lieu, un administrateur de locataire ou un administrateur d'approbation crée les stratégies d'approbation où une gouvernance de provisionnement est nécessaire.

Les stratégies d'approbation sont créées pour des types de stratégie d'approbation ou des éléments spécifiques. Si la stratégie est basée sur un type de stratégie, vous pouvez l'appliquer aux types d'éléments de catalogue correspondants. Par exemple, si une stratégie est basée sur un type de stratégie logicielle, vous pouvez la définir pour les éléments logiciels dans les droits et l'appliquer à tout élément correspondant. Si la stratégie est destinée à un élément spécifique, vous devez l'appliquer uniquement à cet élément. Par exemple, si l'élément est un élément logiciel spécifique, vous devez l'appliquer uniquement à cet élément logiciel de base de données dans le droit d'accès.

Les stratégies peuvent inclure des exigences pré-approbations et post-approbations. Pour les stratégies pré-approbations, la demande doit être approuvée avant que l'élément demandé soit provisionné. Pour les stratégies post-approbations, il est nécessaire que l'approbateur accepte la demande avant que l'élément provisionné ne soit mis à disposition de l'utilisateur y faisant appel.

Les configurations pré-approbations et post-approbations sont composées d'un ou plusieurs niveaux qui déterminent quand la stratégie d'approbation est déclenchée et par qui ou comment la demande est approuvée. Vous pouvez inclure de multiples niveaux. Par exemple, une stratégie d'approbation peut avoir un niveau pour l'approbation du gestionnaire, suivi d'un niveau pour l'approbation financière.

Puis, un administrateur de locataire ou un gestionnaire de groupe d'activité applique les stratégies d'approbation aux services, aux éléments de catalogue et aux actions selon les besoins.

Enfin, lorsqu'un utilisateur de catalogue de services fait appel à un élément auquel une stratégie d'approbation est appliquée, les approbateurs approuvent ou rejettent la demande dans leur onglet **Boîte de réception**, sur la page **Approbations**. L'utilisateur émettant la demande peut contrôler l'état d'approbation d'une demande spécifique dans l'onglet **Demandes**.

Exemples de stratégies d'approbation basées sur le type de stratégie de machine virtuelle

Vous pouvez créer une stratégie d'approbation applicable au même type d'élément de catalogue, mais elle produit des résultats différents lorsqu'un élément est demandé dans le catalogue de services. Selon la manière dont la stratégie d'approbation est définie et appliquée, l'effet sur l'utilisateur du catalogue de services et l'approbateur varie.

Le tableau suivant contient des exemples de différentes stratégies d'approbation, reposant toutes sur le même type de stratégie d'approbation. Ces exemples illustrent certaines configurations possibles des stratégies d'approbation pour accomplir différents types de gouvernance.

Tableau 3-68. Exemples de stratégies d'approbation et résultats

Objectifs de gouvernance	Type de stratégie sélectionnée	Pré ou post-approbation	Quand l'approbation est-elle requise ?	Qui sont les approbateurs ?	Application de la stratégie dans les droits d'accès	Résultats lorsque l'élément est demandé dans le catalogue de services
Le gestionnaire du groupe d'activité doit approuver toute demande de machine virtuelle. La stratégie d'approbation doit être applicable à plusieurs groupes d'activité dans de multiples droits d'accès.	Catalogue de services - Demande d'élément de catalogue - Machine virtuelle	Ajouter à l'onglet Pré-approbation	Sélectionnez Toujours requis.	Sélectionnez Déterminer les approbateurs à partir de la demande. Sélectionnez la condition Groupe d'activité > Gestionnaires > Utilisateurs > gestionnaire. Sélectionnez N'importe qui peut approuver.	Les droits d'accès sont basés sur les groupes d'activité. Cette approbation peut être utilisée dans tout droit d'accès où l'approbation du gestionnaire est requise pour la machine virtuelle.	Lors l'utilisateur de catalogue de services demande une machine virtuelle à laquelle cette approbation est appliquée, le gestionnaire du groupe d'activité doit approuver la demande avant que la machine soit provisionnée.
L'administrateur de l'infrastructure virtuelle doit vérifier le provisionnement de la machine virtuelle et approuver la demande avant que la machine virtuelle soit proposée à l'utilisateur ayant émis la demande.	Catalogue de services - Demande d'élément de catalogue - Machine virtuelle	Ajouter à l'onglet Post-approbation	Sélectionnez Toujours requis.	Sélectionnez Utilisateurs et groupes spécifiques. Sélectionnez votre groupe d'utilisateurs personnalisés d'administrateurs d'infrastructure virtuelle. Sélectionnez N'importe qui peut approuver.	Cette approbation peut être utilisée dans tout droit d'accès où vous souhaitez que l'administrateur d'infrastructure virtuelle vérifie la machine virtuelle du vCenter Server après son provisionnement.	Lors que l'utilisateur de catalogue de services demande une machine virtuelle à laquelle cette approbation est appliquée, la machine virtuelle est provisionnée. Si chaque membre du group d'admin VI approuve la demande, la machine est mise à disposition de l'utilisateur.

Tableau 3-68. Exemples de stratégies d'approbation et résultats (suite)

Objectifs de gouvernance	Type de stratégie sélectionnée	Pré ou post-approbation	Quand l'approbation est-elle requise ?	Qui sont les approbateurs ?	Application de la stratégie dans les droits d'accès	Résultats lorsque l'élément est demandé dans le catalogue de services
Pour gérer les ressources d'infrastructure virtuelle et contrôler les prix, vous ajoutez deux niveaux de pré-approbation : un pour les ressources de la machine et l'autre pour le prix quotidien de la machine.	Catalogue de services - Demande d'élément de catalogue - Machine virtuelle	Ajouter à l'onglet Pré-approbation	Niveau 1 Sélectionnez Requise en fonction des conditions . Configurez les conditions de sorte qu CPU > 6 ou mémoire > 8 ou stockage > 100 Go.	Sélectionnez Déterminer les approbateurs à partir de la demande . Sélectionnez une condition Demandé par > gestionnaire. Sélectionnez . Cliquez sur Propriétés système et sélectionnez CPU. Mémoire et Stockage pour que l'approbateur puisse modifier la valeur à un niveau acceptable.	Cette stratégie d'approbation peut être utilisée dans un droit d'accès où vous souhaitez que le gestionnaire de l'utilisateur ayant émis la demande et un membre du département des finances approuvent la demande.	Lorsque l'utilisateur du catalogue de services demande une machine virtuelle, la demande est évaluée pour déterminer si le CPU, la mémoire ou la taille de stockage dépasse les chiffres spécifiés dans le niveau 1. Si ce n'est pas le cas, la condition de niveau 2 est évaluée. Si la demande ne correspond pas à au moins une des conditions de niveau 1, le gestionnaire doit approuver la demande. Celui-ci a la possibilité de baisser les quantités de configuration demandées et d'approuver ou le gestionnaire rejette la demande.

Tableau 3-68. Exemples de stratégies d'approbation et résultats (suite)

Objectifs de gouvernance	Type de stratégie sélectionnée	Pré ou post-approbation	Quand l'approbation est-elle requise ?	Qui sont les approbateurs ?	Application de la stratégie dans les droits d'accès	Résultats lorsque l'élément est demandé dans le catalogue de services
			Niveau 2 Sélectionnez Requise en fonction des conditions. Configurez la condition Prix >15,00 par jour.	Sélectionnez Utilisateurs et groupes spécifiques. Sélectionnez le groupe personnalisé d'utilisateurs en finance. Sélectionnez N'importe qui peut approuver.		
Dans le cas d'éléments du catalogue de Blueprints paramétrés, un administrateur de cloud doit approuver les demandes de déploiement dans lesquelles un profil de composant de machine vSphere a une valeur de size définie sur Large.	Catalogue de services - Demande d'élément de catalogue - Machine virtuelle	Ajouter à l'onglet Pré-approbation	Niveau 1 Sélectionnez Requise en fonction des conditions. Niveau 2 Sélectionnez l'option Condition unique. Sélectionnez les options Profil de composant > Taille de la machine vSphere. Configurer la condition Taille = Grande.	Sélectionnez Utilisateurs et groupes spécifiques. Sélectionnez les utilisateurs et les groupes qui sont autorisés à approuver la demande. Sélectionnez N'importe qui peut approuver.	Cette stratégie d'approbation peut être utilisée dans un droit lorsque vous voulez qu'un administrateur de cloud approuve la demande de provisionnement.	Lorsque l'utilisateur de catalogue de services demande une machine virtuelle à laquelle cette approbation est appliquée, l'administrateur du cloud doit approuver la demande avant que la machine soit provisionnée.

Exemple d'actions avec des stratégies d'approbation dans un déploiement composite

Lorsque vous appliquez des stratégies d'approbation à des actions qui peuvent s'exécuter sur plusieurs composants d'un Blueprint composite, le processus d'approbation varie en fonction de la manière dont le droit est configuré et dont les stratégies d'approbation s'appliquent.

Cet exemple utilise des détails spécifiques pour créer le Blueprint, puis pour appliquer des stratégies d'approbation aux actions que vous pouvez exécuter à partir du catalogue de services sur le Blueprint provisionné dans plusieurs droits. Le Blueprint est un Blueprint composite qui inclut un autre Blueprint. Les actions utilisées permettent de détruire les éléments provisionnés, de détruire un déploiement pour les Blueprints et de détruire une machine virtuelle pour la machine. Le résultat inclut ce qui est détruit et le moment où les stratégies d'approbation déclenchent les demandes d'approbation.

Exemple de Blueprint

Dans cet exemple, vous configurez un Blueprint qui inclut un Blueprint imbriqué avec une machine virtuelle.

- Blueprint 1 - Blueprint d'intégration continue
 - Blueprint 2 - Blueprint de pré-production
 - Machine virtuelle 1 - Machine virtuelle vSphere TestAsAService

Stratégies d'approbation pour actions de destruction

Vous configurez les deux stratégies d'approbation pour détruire les éléments provisionnés. Destruction A - L'action sur le déploiement peut être exécutée sur le Blueprint 1 ou le Blueprint 2 dans cet exemple. Destruction A - L'action sur la machine virtuelle peut être exécutée sur la machine virtuelle 1. Vous créez les stratégies d'approbation de façon à les appliquer aux actions dans le droit d'accès.

Nom de la stratégie d'approbation	Type de stratégie d'approbation
Stratégie d'approbation A	Catalogue de services - Demande d'action sur les ressources - Détruire - Déploiement
Stratégie d'approbation B	Catalogue de services - Demande d'action sur les ressources - Détruire - Machine virtuelle

Droits d'accès et stratégies d'approbation appliquées aux actions

Vous configurez trois droits d'accès. Chaque droit d'accès inclut le Blueprint composite. Dans chaque droit d'accès, vous ajoutez les actions de destruction et vous appliquez les stratégies d'approbation.

Nom du droit	Action autorisée sur la machine provisionnée	Stratégie d'approbation appliquée
Droit d'accès 1	Détruire - Déploiement	Stratégie d'approbation A
Droit d'accès 2	Détruire - Machine virtuelle	Stratégie d'approbation B
Droit d'accès 3	Détruire - Déploiement	Stratégie d'approbation A
	Détruire - Machine virtuelle	Stratégie d'approbation B

Actions sur les utilisateurs dans le catalogue de services

Lorsque l'utilisateur du catalogue de services exécute l'action, les Blueprints ou les machines sont détruites en fonction de l'élément sur lequel l'utilisateur a exécuté l'action.

Action sur les utilisateurs dans le catalogue de services	Action sélectionnée	Blueprints ou machines détruits
Action 1	Détruire - Action sur le déploiement exécutée sur le Blueprint 1 - Blueprint d'intégration continue	Blueprint 1, Blueprint 2 et machine virtuelle 1
Action 2	Détruire - Action sur le déploiement exécutée sur le Blueprint 2 imbriqué - Blueprint de pré-production	Blueprint 2 et machine virtuelle 1
Action 3	Détruire - L'action sur la machine virtuelle s'exécute sur la machine qui se trouve dans un déploiement, Machine virtuelle 1 - Machine virtuelle vSphere TestAsAService	Machine virtuelle 1

Stratégies d'approbation appliquées aux actions dans les droits d'accès

Vous appliquez les stratégies d'approbation, les approbateurs reçoivent une demande d'approbation en fonction de la machine ou du Blueprint sur lequel l'utilisateur de votre catalogue de services a exécuté l'action.

Nom du droit	Stratégie d'approbation sur les actions	Action sur l'utilisateur	Demande d'approbation déclenchée	En cas d'approbation, machines ou Blueprints détruits
Droit d'accès 1 - Destruction de la stratégie d'approbation de déploiement	Stratégie A (destruction de stratégie d'approbation de déploiement) sur destruction - Action sur le déploiement uniquement	Action 1 (Exécution de destruction - Action sur le déploiement sur le Blueprint 1)	Les demandes d'approbation sont déclenchées pour le Blueprint 1 uniquement	Blueprint 1, Blueprint 2 et machine virtuelle 1
		Action 2 (Exécution de destruction - Action sur le déploiement sur le Blueprint 2)	Les demandes d'approbation sont déclenchées pour le Blueprint 2 uniquement	Blueprint 2 et machine virtuelle 1
		Action 3 (Détruire - L'action sur la machine virtuelle s'exécute sur la machine virtuelle 1)	Aucune demande d'approbation n'est déclenchée	Machine virtuelle 1
Droit d'accès 2	Stratégie B (Destruction - Stratégie de machine virtuelle) sur la destruction - Action sur la machine virtuelle uniquement	Action 1 (Exécution de destruction - Action sur le déploiement sur le Blueprint 1)	Aucune demande d'approbation n'est déclenchée	Blueprint 1, Blueprint 2 et machine virtuelle 1
		Action 2 (Exécution de destruction - Action sur le déploiement sur le Blueprint 2)	Aucune demande d'approbation n'est déclenchée	Blueprint 2 et machine virtuelle 1

Nom du droit	Stratégie d'approbation sur les actions	Action sur l'utilisateur	Demande d'approbation déclenchée	En cas d'approbation, machines ou Blueprints détruits
		Action 3 (Détruire - L'action sur la machine virtuelle s'exécute sur la machine virtuelle 1)	Les demandes d'approbation sont déclenchées pour la machine virtuelle 1 uniquement	Machine virtuelle 1
Droit d'accès 3	Stratégie A (Destruction de stratégie d'approbation de déploiement) sur la destruction - Action sur le déploiement et stratégie B (Destruction - Stratégie de machine virtuelle) sur la destruction - Action sur la machine virtuelle	Action 1 (Exécution de destruction - Action sur le déploiement sur le Blueprint 1)	Les demandes d'approbation sont déclenchées pour le Blueprint 1 uniquement	Blueprint 1, Blueprint 2 et machine virtuelle 1
		Action 2 (Exécution de destruction - Action sur le déploiement sur le Blueprint 2)	Les demandes d'approbation sont déclenchées pour le Blueprint 2 uniquement	Blueprint 2 et machine virtuelle 1
		Action 3 (Détruire - L'action sur la machine virtuelle s'exécute sur la machine virtuelle 1)	Les demandes d'approbation sont déclenchées pour la machine virtuelle 1 uniquement	Machine virtuelle 1

Exemple d'une stratégie d'approbation dans de multiples droits d'accès

Si vous appliquez une stratégie d'approbation à un élément qui participe à plusieurs droits d'accès accordés aux mêmes utilisateurs d'un groupe d'activité, cette stratégie est déclenchée sur l'élément, y compris dans le service pour lequel elle ne s'applique pas explicitement au droit d'accès.

Par exemple, créez les Blueprints, services, stratégies d'approbation et droits d'accès suivants :

Blueprints

- Machine virtuelle vSphere RHEL.
- Le test de l'environnement QE inclut une machine virtuelle vSphere RHEL.
- La formation à l'environnement QE inclut une machine virtuelle vSphere RHEL.

Services

- Le Blueprint de test de l'environnement QE est associé au service de test.
- Le Blueprint de formation à l'environnement QE est associé au service de formation.

Droits

- Droit d'accès 1
- Droit d'accès 2

Tableau 3-69. Configurations des droits

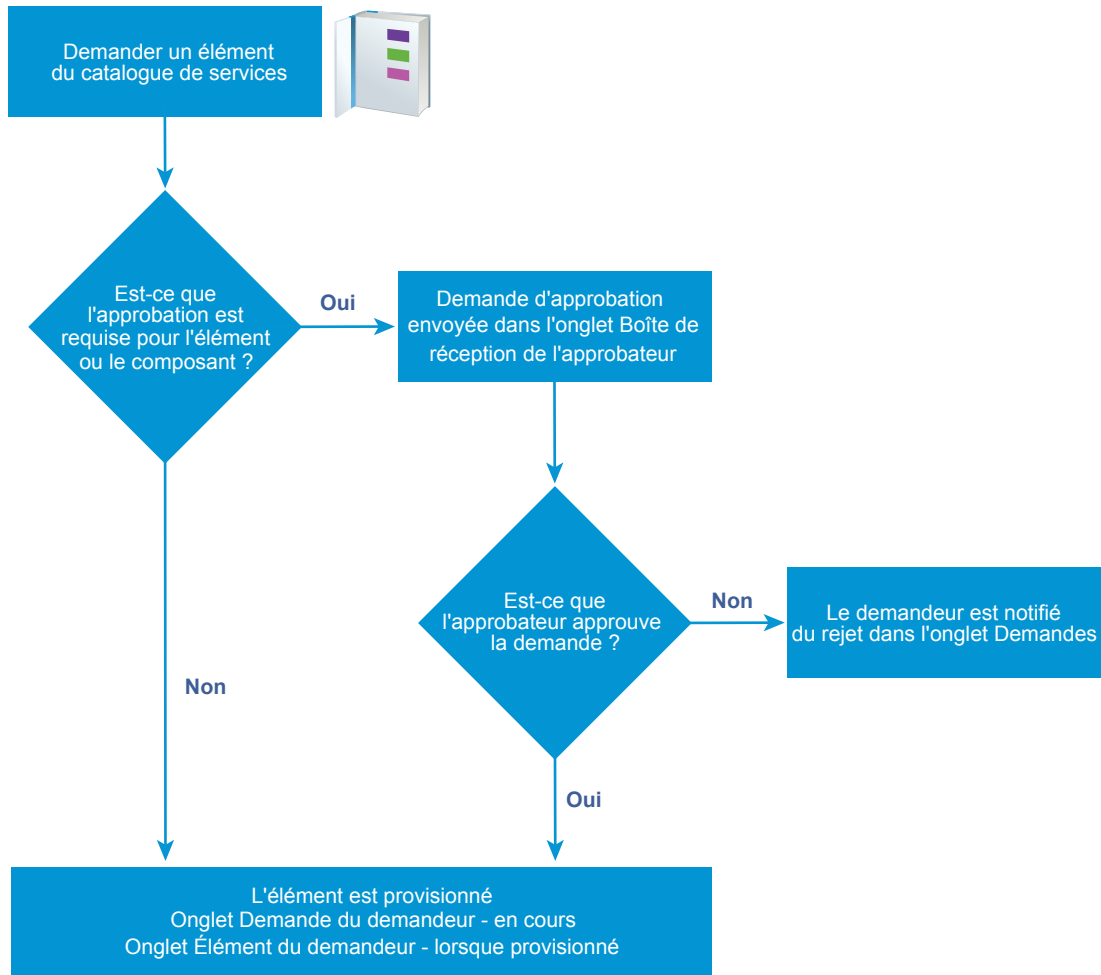
Nom du droit	Groupe d'activité	Service autorisé	Élément autorisé
Droit d'accès 1	QE	Test	Demande d'élément de catalogue - Machine virtuelle appliquée à un composant de machine virtuelle
Droit d'accès 2	QE	Formation	

Résultats

Lorsque l'utilisateur sélectionne une formation à l'environnement QE, la stratégie d'approbation est déclenchée pour la machine virtuelle vSphere RHEL, car il s'agit d'un Blueprint reposant sur un composant de machine virtuelle utilisé dans le Blueprint de formation à l'environnement QE.

Traitement des stratégies d'approbation dans le catalogue de services

Lorsqu'un utilisateur demande un élément du catalogue de services comportant une stratégie d'approbation, la demande est traitée par l'approbateur et l'utilisateur demandeur, selon le workflow suivant :



Créer une stratégie d'approbation

Les administrateurs de locataire et les administrateurs d'approbations peuvent définir des stratégies d'approbation et les utiliser dans les droits d'accès. Vous pouvez configurer les stratégies d'approbation avec plusieurs niveaux destinés aux événements survenant avant l'approbation et après l'approbation.

Si vous modifiez un paramètre du Blueprint d'un composant logiciel et qu'une stratégie d'approbation utilise ce paramètre pour déclencher une demande d'approbation, la stratégie peut ne pas fonctionner comme prévu. Si vous devez modifier un paramètre de composant, vérifiez que les modifications apportées sont sans incidence sur les stratégies d'approbation.

Prérequis

Connectez-vous à la console vRealize Automation en tant qu'**administrateur de locataire** ou **administrateur d'approbation**.

Procédure

1 Spécifier des informations de stratégie d'approbation

Lorsque vous créez une stratégie d'approbation, définissez le type, le nom, la description et l'état de stratégie d'approbation.

2 Créer un niveau d'approbation

Lorsque vous créez une stratégie d'approbation, vous pouvez ajouter des niveaux avant et après approbation.

3 Configurer un formulaire d'approbation pour inclure des propriétés système et des propriétés personnalisées

Vous pouvez ajouter des propriétés système et des propriétés personnalisées à un formulaire d'approbation. Cela permet aux approbateurs de modifier les valeurs des propriétés système pour les paramètres des ressources de machine, tels que le CPU, le bail ou la mémoire, et des propriétés personnalisées avant de clôturer une demande d'approbation.

4 Paramètres de stratégie d'approbation

Lorsque vous créez une stratégie d'approbation, vous configurez plusieurs options qui déterminent à quel moment un élément demandé par les utilisateurs d'un catalogue de services doit être approuvé. L'approbation peut être requise avant que la demande ne débute le provisionnement, ou après que l'élément soit provisionné mais avant qu'il ne soit mis à disposition de l'utilisateur à l'origine de la demande.

Spécifier des informations de stratégie d'approbation

Lorsque vous créez une stratégie d'approbation, définissez le type, le nom, la description et l'état de stratégie d'approbation.

Prérequis

Connectez-vous à la console vRealize Automation en tant qu'**administrateur de locataire** ou **administrateur d'approbation**.

Procédure

- 1 Sélectionnez **Administration > Stratégies d'approbation**.
- 2 Cliquez sur l'icône **Nouveau (+)**.

3 Sélectionnez un type de stratégie pour votre composant logiciel.

Option	Description
Sélectionnez un type de stratégie d'approbation	<p>Créez une stratégie d'approbation basée sur le type de demande de stratégie. Sélectionnez cette option pour définir une stratégie d'approbation applicable à tous les éléments de catalogue de ce type. Le type de demande peut être une demande générique, une demande d'élément de catalogue ou une demande d'action sur les ressources.</p> <p>Les options de configuration de conditions disponibles varient selon le type. Plus le type est spécifique, plus les champs de configuration sont spécifiques. Par exemple, Catalogue de services - Demande d'élément de catalogue fournit uniquement les champs qui sont communs à toutes les demandes d'éléments de catalogue, tandis que Catalogue de services - Demande d'élément de catalogue - Machine virtuelle inclut également les options communes et les options spécifiques aux machines virtuelles.</p> <p>Le type de demande limite les éléments de catalogue ou les actions auxquels vous pouvez appliquer la stratégie d'approbation.</p>
Sélectionner un élément	<p>Créez une stratégie d'approbation basée sur un élément spécifique. Sélectionnez cette option pour définir une stratégie d'approbation applicable à des éléments spécifiques qui ne sont pas disponibles en tant qu'éléments individuels dans le catalogue de services, mais uniquement dans le cadre du déploiement d'une machine ou de tout autre déploiement. Par exemple, des composants logiciels.</p> <p>Les champs de configuration de conditions disponibles sont spécifiques à l'élément et peuvent être plus détaillés que les critères offerts pour un élément de type de stratégie.</p>
Liste	<p>Répertorie les types de stratégie ou les éléments de catalogue disponibles. Triez les colonnes pour rechercher un élément ou un type spécifique.</p>

4 Cliquez sur **OK**.

5 Entrez un nom et, éventuellement, une description.

6 Sélectionnez l'état de la stratégie dans le menu déroulant **Statut**.

Option	Description
Brouillon	Enregistre la stratégie d'approbation dans un état modifiable.
Actif	Enregistre la stratégie d'approbation dans un état de lecture seule que vous pouvez utiliser dans une autorisation.
Inactif	Enregistre la stratégie d'approbation dans un état de lecture seule que vous ne pouvez pas utiliser dans une autorisation avant d'avoir activé la stratégie.

Suivant

Créez les niveaux d'avant approbation et d'après approbation.

Créer un niveau d'approbation

Lorsque vous créez une stratégie d'approbation, vous pouvez ajouter des niveaux avant et après approbation.

Vous pouvez créer plusieurs niveaux d'approbation pour une stratégie d'approbation. Lorsque l'utilisateur d'un catalogue de services demande un élément auquel est appliquée une stratégie d'approbation à plusieurs niveaux, chaque premier niveau doit être accepté avant que la demande d'approbation ne puisse être envoyée à l'approbateur suivant. Reportez-vous à [Utilisation de stratégies d'approbation](#).

Prérequis

[Spécifier des informations de stratégie d'approbation](#).

Procédure

- 1 Dans l'onglet **Pré-approbation** ou **Post-approbation**, cliquez sur l'icône **Nouveau** (+).
- 2 Entrez un nom et, éventuellement, une description.
- 3 Sélectionnez une condition d'approbation.

Option	Description
Toujours requise	La stratégie d'approbation est déclenchée pour chaque demande.
Requise en fonction des conditions	<p>La stratégie d'approbation est basée sur une ou plusieurs clauses de condition. Si vous sélectionnez cette option, vous devez créer les conditions. Lorsque cette stratégie d'approbation est appliquée aux services, aux éléments de catalogue ou aux actions d'une autorisation éligibles, les conditions sont alors évaluées. Si les conditions sont vraies, la demande doit être approuvée conformément à la méthode spécifiée par l'approbateur avant d'être provisionnée. Si les conditions sont fausses, la demande est provisionnée sans nécessiter d'approbation. Par exemple, toute demande de machine virtuelle comprenant au moins 4 CPU doit être approuvée par l'administrateur de l'infrastructure virtuelle.</p> <p>La disponibilité des champs sur lesquels doivent se baser les conditions est déterminée par le type de stratégie d'approbation ou l'élément de catalogue sélectionné.</p> <p>Les valeurs que vous entrez pour les conditions sont sensibles à la casse.</p> <p>Afin de configurer plusieurs clauses de condition, sélectionnez l'opération booléenne pour ces clauses.</p>

- 4 Sélectionnez les approbateurs.

Option	Action
Des utilisateurs et des groupes spécifiques	Envoie la demande d'approbation aux utilisateurs sélectionnés.
Déterminer les approbateurs à partir de la demande	Envoie la demande d'approbation aux utilisateurs en fonction des conditions définies.
Utiliser l'abonnement à l'événement	<p>Traite la demande d'approbation en fonction des abonnements à l'événement définis.</p> <p>L'abonnement à un workflow doit être défini dans Administration > Événements > Abonnements. Les abonnements à un workflow applicables s'effectuent avant approbation et après approbation.</p>

5 Spécifiez l'auteur de l'approbation de la demande ou de l'action.

Option	Description
N'importe qui peut approuver	Un seul des approbateurs doit approuver la demande avant qu'elle ne soit traitée. Lorsque l'élément est demandé dans le catalogue de services, les demandes d'approbation sont envoyées à tous les approbateurs. Si un approbateur approuve la demande, celle-ci est approuvée et la demande d'approbation est supprimée de la boîte de réception des autres approbateurs.
Tous doivent approuver	Tous les approbateurs spécifiés doivent approuver la demande avant qu'elle ne soit traitée.

6 Ajoutez des propriétés à un formulaire d'approbation ou enregistrez le niveau.

- Pour ajouter des propriétés au formulaire, cliquez sur **Propriétés du système** ou **Propriétés personnalisées**.
- Pour enregistrer le niveau, cliquez sur **OK**.

Suivant

Pour ajouter des propriétés au formulaire d'approbation, reportez-vous à [Configurer un formulaire d'approbation pour inclure des propriétés système et des propriétés personnalisées](#).

Configurer un formulaire d'approbation pour inclure des propriétés système et des propriétés personnalisées

Vous pouvez ajouter des propriétés système et des propriétés personnalisées à un formulaire d'approbation. Cela permet aux approbateurs de modifier les valeurs des propriétés système pour les paramètres des ressources de machine, tels que le CPU, le bail ou la mémoire, et des propriétés personnalisées avant de clôturer une demande d'approbation.

Les propriétés système disponibles dépendent du type de stratégie d'approbation et du mode de configuration du Blueprint. Pour certaines propriétés, le champ configuré dans le Blueprint doit inclure une valeur minimale et une valeur maximale avant que la propriété ne s'affiche dans la liste des propriétés système.

Les propriétés personnalisées peuvent être ajoutées lorsque vous ajoutez le niveau d'approbation. Si une propriété personnalisée est configurée et incluse dans un Blueprint, les propriétés personnalisées que vous ajoutez au formulaire d'approbation remplacent toutes les autres instances de cette propriété, notamment dans les Blueprints, les groupes de propriétés ou les points de terminaison.

L'approbateur peut modifier les propriétés sélectionnées ou configurées dans le formulaire d'approbation.

Prérequis

- Connectez-vous à la console vRealize Automation en tant qu'**administrateur de locataire** ou **administrateur d'approbation**.
- [Créer un niveau d'approbation](#).

Procédure

- 1 Dans l'onglet **Pré-approbation** ou **Post-approbation**, cliquez sur l'icône **Nouveau** (+).

2 Cliquez sur l'onglet **Propriétés du système**.

3 Cochez la case de chaque propriété système que vous souhaitez que l'approbateur configure lors du processus d'approbation.

4 Configurez les propriétés personnalisées.

Ajoutez une ou plusieurs propriétés personnalisées que vous souhaitez que l'approbateur configure lors du processus d'approbation.

a Cliquez sur l'onglet **Propriétés personnalisées**.

b Cliquez sur l'icône **Nouveau** (+).

c Entrez les valeurs de propriétés personnalisées.

Option	Description
Nom	Entrez le nom de la propriété.
Label	Entrez l'étiquette qui est présentée à l'approbateur sur le formulaire d'approbation.
Description	Entrez les informations complémentaires pour l'approbateur. Ces informations apparaissent dans l'info-bulle du champ sur le formulaire.

d Cliquez sur **Enregistrer**.

e Pour supprimer plusieurs propriétés personnalisées, sélectionnez les lignes correspondantes, puis cliquez sur **Supprimer**.

5 Cliquez sur **OK**.

Suivant

- Ajoutez des niveaux avant approbation ou après approbation.
- Enregistrez la stratégie d'approbation. La stratégie doit être activée pour s'appliquer aux services, aux éléments ou aux actions dans les **Droits d'accès**.

Paramètres de stratégie d'approbation

Lorsque vous créez une stratégie d'approbation, vous configurez plusieurs options qui déterminent à quel moment un élément demandé par les utilisateurs d'un catalogue de services doit être approuvé.

L'approbation peut être requise avant que la demande ne débute le provisionnement, ou après que l'élément soit provisionné mais avant qu'il ne soit mis à disposition de l'utilisateur à l'origine de la demande.

Sélectionnez **Administration > Stratégies d'approbation**. Cliquez sur **Nouveau**.

■ Paramètres de type de stratégie d'approbation

Le type de stratégie d'approbation détermine le mode de configuration de la stratégie d'approbation et les éléments ou actions auxquels vous pouvez l'appliquer dans le droit. Lorsque vous ajoutez des niveaux d'approbation, le type de stratégie ou d'élément affecte la nature des champs disponibles pour la création des conditions des niveaux d'approbation.

- [Ajouter des paramètres de stratégie d'approbation](#)

Vous devez configurer les informations de base concernant la stratégie d'approbation, notamment son état, afin de pouvoir la gérer.

- [Ajouter des informations de niveau aux paramètres de stratégie d'approbation](#)

Un niveau d'approbation comprend les conditions qui déclenchent une procédure d'approbation lorsque l'utilisateur du catalogue de services demande l'élément ainsi que toute propriété système et personnalisée que vous souhaitez y inclure. Une fois émises, les demandes d'approbation sont envoyées aux approbateurs désignés.

- [Ajouter des propriétés système aux paramètres de stratégie d'approbation](#)

Vous avez sélectionné des propriétés du système que vous souhaitez ajouter au formulaire d'approbation et autorisez l'approbateur à modifier la valeur.

- [Ajouter des propriétés personnalisées aux paramètres de stratégie d'approbation](#)

Vous configurez des propriétés personnalisées que vous souhaitez ajouter au formulaire d'approbation pour autoriser l'approbateur à modifier la valeur.

Paramètres de type de stratégie d'approbation

Le type de stratégie d'approbation détermine le mode de configuration de la stratégie d'approbation et les éléments ou actions auxquels vous pouvez l'appliquer dans le droit. Lorsque vous ajoutez des niveaux d'approbation, le type de stratégie ou d'élément affecte la nature des champs disponibles pour la création des conditions des niveaux d'approbation.

Sélectionnez **Administration > Stratégies d'approbation**. Cliquez sur **Nouveau**.

Tableau 3-70. Options Type de stratégie d'approbation

Option	Description
Sélectionnez un type de stratégie d'approbation	<p>Créez une stratégie d'approbation basée sur le type de demande de stratégie.</p> <p>Sélectionnez cette option pour définir une stratégie d'approbation applicable à tous les éléments de catalogue de ce type. Le type de demande peut être une demande générique, une demande d'élément de catalogue ou une demande d'action sur les ressources.</p> <p>Les options de configuration de conditions disponibles varient selon le type. Plus le type est spécifique, plus les champs de configuration sont spécifiques. Par exemple, Catalogue de services - Demande d'élément de catalogue fournit uniquement les champs qui sont communs à toutes les demandes d'éléments de catalogue, tandis que Catalogue de services - Demande d'élément de catalogue - Machine virtuelle inclut également les options communes et les options spécifiques aux machines virtuelles.</p> <p>Le type de demande limite les éléments de catalogue ou les actions auxquels vous pouvez appliquer la stratégie d'approbation.</p>
Sélectionner un élément	<p>Créez une stratégie d'approbation basée sur un élément spécifique.</p> <p>Sélectionnez cette option pour définir une stratégie d'approbation applicable à des éléments spécifiques qui ne sont pas disponibles en tant qu'éléments individuels dans le catalogue de services, mais uniquement dans le cadre du déploiement d'une machine ou de tout autre déploiement. Par exemple, des composants logiciels.</p> <p>Les champs de configuration de conditions disponibles sont spécifiques à l'élément et peuvent être plus détaillés que les critères offerts pour un élément de type de stratégie.</p>
Liste	<p>Répertorie les types de stratégie ou les éléments de catalogue disponibles.</p> <p>Triez les colonnes pour rechercher un élément ou un type spécifique.</p>

Ajouter des paramètres de stratégie d'approbation

Vous devez configurer les informations de base concernant la stratégie d'approbation, notamment son état, afin de pouvoir la gérer.

Pour définir les informations de base relatives à la stratégie d'approbation, sélectionnez **Administration > Stratégies d'approbation**. Cliquez sur **Nouveau**. Sélectionnez le type de stratégie et cliquez sur **OK**.

Tableau 3-71. Options de la stratégie d'approbation

Option	Description
Nom	Nom qui s'affiche lorsque vous appliquez la stratégie d'approbation à un droit d'accès.
Description	Fournissez une description détaillée de la manière dont la stratégie d'approbation est construite. Ces informations vous aideront à gérer vos stratégies d'approbation.
État	<p>Les valeurs possibles sont les suivantes :</p> <ul style="list-style-type: none"> ■ Brouillon. La stratégie d'approbation n'est pas prête à être appliquée à des droits d'accès. Après avoir activé une stratégie, vous ne pouvez plus la faire revenir à l'état de brouillon. ■ Actif. La stratégie d'approbation est prête à être appliquée à des droits d'accès. ■ Inactif. La stratégie d'approbation n'est pas prête à être appliquée à des droits d'accès. Si la stratégie n'a pas été appliquée aux droits d'accès et vous la rendez inactive, vous pouvez la supprimer, mais ne pouvez pas la réactiver. Si la stratégie a été appliquée et vous la rendez inactive, les éléments auxquels elle s'applique doivent être liés à une autre stratégie, sinon ils seront dissociés. Les éléments et les actions dissociés sont toujours accessibles aux utilisateurs, mais aucune stratégie d'approbation ne leur est appliquée.
Type de stratégie	<p>Affiche le type de demande de stratégie d'approbation.</p> <p>Si vous avez sélectionné un élément de catalogue sur lequel baser la stratégie d'approbation, le type de demande associé est affiché.</p>
Élément	<p>Affiche l'élément de catalogue sélectionné.</p> <p>Si vous avez sélectionné un type de demande sur lequel baser la stratégie d'approbation, le champ est vide.</p>
Dernière mise à jour par	Nom de l'utilisateur ayant apporté des changements à la stratégie d'approbation.
Dernière mise à jour le	Date de la dernière modification de la stratégie d'approbation.
Niveau de pré-approbation	Pour exiger une approbation avant le provisionnement des éléments demandés ou l'exécution des actions demandées, configurez une ou plusieurs conditions qui déclenchent un processus d'approbation au moment où l'utilisateur du catalogue de services demande l'élément.

Tableau 3-71. Options de la stratégie d'approbation (suite)

Option	Description
Niveau de post-approbation	<p>Pour exiger une approbation après le provisionnement de l'élément, mais avant que l'élément provisionné ou modifié soit mis à disposition de l'utilisateur du catalogue de services ayant fait la demande, configurez une ou plusieurs conditions qui déclenchent un processus d'approbation.</p> <p>Par exemple, l'administrateur d'infrastructure virtuelle vérifie que la machine virtuelle est opérationnelle avant de la mettre à disposition de l'utilisateur du catalogue de services.</p>
Afficher les droits d'accès liés	<p>Affiche tous les droits d'accès pour lesquels la stratégie d'approbation est appliquée aux services, aux éléments de catalogue ou aux actions. Vous pouvez lier les éléments d'un droit d'accès à une stratégie différente.</p> <p>Cette option est uniquement disponible lorsque vous affichez une stratégie d'approbation active.</p>

Ajouter des informations de niveau aux paramètres de stratégie d'approbation

Un niveau d'approbation comprend les conditions qui déclenchent une procédure d'approbation lorsque l'utilisateur du catalogue de services demande l'élément ainsi que toute propriété système et personnalisée que vous souhaitez y inclure. Une fois émises, les demandes d'approbation sont envoyées aux approbateurs désignés.

Pour définir les informations de base relatives à la stratégie d'approbation, sélectionnez **Administration > Stratégies d'approbation**. Cliquez sur **Nouveau**. Sélectionnez le type de stratégie et cliquez sur **OK**.

Dans l'onglet Pré-approbation ou Post-approbation, cliquez sur l'icône **Nouveau** (+).

Vous priorisez les niveaux selon l'ordre dans lequel vous souhaitez qu'ils soient traités. Lorsqu'une stratégie d'approbation est déclenchée, si le premier niveau d'approbation est rejeté, la demande est refusée.

Tableau 3-72. Options Informations sur le niveau

Option	Description
Nom	<p>Entrez un nom.</p> <p>Le nom du niveau apparaît lorsque vous vérifiez les demandes avec les stratégies d'approbation.</p>
Description	<p>Entrez une description pour le niveau.</p> <p>Par exemple, CPU>4 pour admin. infrastructure virtuelle</p>
Quand l'approbation est-elle requise ?	Indiquez le moment auquel la stratégie d'approbation doit se déclencher.

Tableau 3-72. Options Informations sur le niveau (suite)

Option	Description
Toujours requise	<p>La stratégie d'approbation est déclenchée pour chaque demande.</p> <p>Si vous sélectionnez cette option et que vous appliquez cette stratégie d'approbation aux services, aux éléments de catalogue ou aux actions d'une autorisation éligibles, la demande doit alors être approuvée selon la méthode spécifiée par l'approbateur avant d'être provisionnée. Par exemple, toutes les demandes doivent être approuvées par le gestionnaire de l'utilisateur qui fait la demande.</p>
Requise en fonction des conditions	<p>La stratégie d'approbation est basée sur une ou plusieurs clauses de condition.</p> <p>Si vous sélectionnez cette option, vous devez créer les conditions. Lorsque cette stratégie d'approbation est appliquée aux services, aux éléments de catalogue ou aux actions d'une autorisation éligibles, les conditions sont alors évaluées. Si les conditions sont vraies, la demande doit être approuvée conformément à la méthode spécifiée par l'approbateur avant d'être provisionnée. Si les conditions sont fausses, la demande est provisionnée sans nécessiter d'approbation. Par exemple, toute demande de machine virtuelle comprenant au moins 4 CPU doit être approuvée par l'administrateur de l'infrastructure virtuelle.</p> <p>La disponibilité des champs sur lesquels doivent se baser les conditions est déterminée par le type de stratégie d'approbation ou l'élément de catalogue sélectionné.</p> <p>Les valeurs que vous entrez pour les conditions sont sensibles à la casse.</p> <p>Afin de configurer plusieurs clauses de condition, sélectionnez l'opération booléenne pour ces clauses.</p> <ul style="list-style-type: none"> ■ Tous les éléments suivants. L'approbation est déclenchée lorsque toutes les conditions sont vraies. Il s'agit d'un opérateur ET booléen entre chaque clause. ■ L'un des éléments suivants. Le niveau d'approbation est déclenché lorsque l'une des clauses au moins est vraie. Il s'agit d'un opérateur OU booléen entre chaque clause. ■ Pas les éléments suivants. Le niveau d'approbation est déclenché si aucune des conditions n'est vraie. Il s'agit d'un opérateur NON booléen entre chaque clause.
Approbateurs	Sélectionnez la méthode d'approbation.
Utilisateurs et groupes spécifiques	<p>Envoie la demande d'approbation aux utilisateurs sélectionnés. Sélectionnez les utilisateurs ou groupes d'utilisateurs qui doivent approuver la demande de catalogue de services avant qu'elle ne soit provisionnée ou qu'une action ne soit exécutée. Par exemple, la demande est transmise au groupe d'administrateurs de l'infrastructure virtuelle avec l'option N'importe qui peut approuver sélectionnée.</p>

Tableau 3-72. Options Informations sur le niveau (suite)

Option	Description
Déterminer les utilisateurs à partir de la demande	<p>Envoie la demande d'approbation aux utilisateurs en fonction des conditions définies.</p> <p>Par exemple, si vous appliquez cette stratégie d'approbation à plusieurs groupes d'activité et si vous souhaitez que le gestionnaire de groupe d'activité approuve la demande, sélectionnez Groupe d'activité > Consommateur > Utilisateurs > Gestionnaire.</p>
Utiliser l'abonnement à l'événement	<p>Traite la demande d'approbation en fonction des abonnements à l'événement définis.</p> <p>L'abonnement à un workflow doit être défini dans Administration > Événements > Abonnements. Les abonnements à un workflow applicables s'effectuent avant approbation et après approbation.</p>
N'importe qui peut approuver	<p>Un seul des approbateurs doit approuver la demande avant qu'elle ne soit traitée.</p> <p>Lorsque l'élément est demandé dans le catalogue de services, les demandes d'approbation sont envoyées à tous les approbateurs. Si un approbateur approuve la demande, celle-ci est approuvée et la demande d'approbation est supprimée de la boîte de réception des autres approbateurs.</p> <p>Si le premier approbateur rejette la demande, l'utilisateur qui fait la demande est informé du refus et la demande d'approbation est supprimée de la boîte de réception des autres approbateurs.</p> <p>Si le premier approbateur approuve et que la demande d'approbation est ouverte dans la console du second approbateur, l'approbateur n'est pas autorisé à soumettre la demande d'approbation. Elle est considérée comme terminée à l'intervention du premier approbateur.</p> <p>Si vous sélectionnez Utilisateurs et groupes spécifiques ou Déterminer les approbateurs à partir de la demande et qu'il existe plusieurs approbateurs, cette option fait partie des options supplémentaires. S'il n'existe qu'un seul approbateur, cette option ne s'applique pas.</p>
Tous doivent approuver	<p>Tous les approbateurs spécifiés doivent approuver la demande avant qu'elle ne soit traitée.</p> <p>Si vous sélectionnez Utilisateurs et groupes spécifiques ou Déterminer les approbateurs à partir de la demande et qu'il existe plusieurs approbateurs, cette option fait partie des options supplémentaires. S'il n'existe qu'un seul approbateur, cette option ne s'applique pas.</p>

Ajouter des propriétés système aux paramètres de stratégie d'approbation

Vous avez sélectionné des propriétés du système que vous souhaitez ajouter au formulaire d'approbation et autorisez l'approbateur à modifier la valeur.

Par exemple, pour une approbation de machine virtuelle, sélectionnez CPU si vous souhaitez autoriser l'approbateur à modifier une demande de 6 CPU à 4 CPU.

Pour sélectionner des propriétés système, sélectionnez **Administration > Stratégies d'approbation**. Cliquez sur **Nouveau**. Sélectionnez le type de stratégie et cliquez sur **OK**. Dans l'onglet Pré-approbation ou Post-approbation, cliquez sur l'icône **Nouveau (+)** et cliquez sur l'onglet **Propriétés du système**.

Tableau 3-73. Options Propriétés système

Option	Description
Propriétés	<p>La liste des propriétés système disponibles dépend du type de demande ou de l'élément de catalogue sélectionné, ainsi que de l'existence ou non de propriétés système pour l'élément.</p> <p>Certaines propriétés sont disponibles uniquement lorsque le Blueprint est configuré d'une certaine manière. Par exemple, CPU. Le Blueprint auquel vous appliquez la stratégie d'approbation avec la propriété système CPU doit être défini sous forme de plage de valeurs. Par exemple, le nombre minimal de CPU est 2 et le nombre maximal est 8.</p>

Ajouter des propriétés personnalisées aux paramètres de stratégie d'approbation

Vous configurez des propriétés personnalisées que vous souhaitez ajouter au formulaire d'approbation pour autoriser l'approbateur à modifier la valeur.

Par exemple, pour une approbation de machine virtuelle, ajoutez **VMware.VirtualCenter.Folder** si vous souhaitez autoriser l'approbateur à spécifier le dossier dans lequel la machine est ajoutée dans vCenter Server.

Vous pouvez aussi ajouter une propriété personnalisée spécifique à ce formulaire de stratégie d'approbation.

Pour sélectionner des propriétés système, sélectionnez **Administration > Stratégies d'approbation**. Cliquez sur **Nouveau**. Sélectionnez le type de stratégie et cliquez sur **OK**. Dans l'onglet Pré-approbation ou Post-approbation, cliquez sur l'icône **Nouveau (+)** et cliquez sur l'onglet **Propriétés personnalisées**.

Tableau 3-74. Propriétés personnalisées

Option	Description
Nom	Entrez le nom de la propriété.
Étiquette	Entrez l'étiquette qui est présentée à l'approbateur sur le formulaire d'approbation.
Description	<p>Entrez les informations complémentaires pour l'approbateur.</p> <p>Ces informations apparaissent dans l'info-bulle du champ sur le formulaire.</p>

Modifier une stratégie d'approbation

Vous ne pouvez pas modifier une stratégie d'approbation active ou inactive. Vous devez créer une copie de la stratégie d'approbation d'origine et remplacer la stratégie qui ne produit pas les résultats souhaités. Les stratégies d'approbation actives et inactives sont en mode de lecture seule. En revanche, vous pouvez modifier une stratégie d'approbation qui est à l'état de brouillon.


Lorsque vous copiez la stratégie d'approbation, la nouvelle stratégie dépend du type de la stratégie d'origine. Vous pouvez modifier tous les attributs, à l'exception du type de stratégie. Procédez ainsi lorsque vous souhaitez modifier les niveaux d'approbation afin de changer, d'ajouter ou de supprimer des niveaux, ou afin d'ajouter des propriétés système ou des propriétés personnalisées aux formulaires.

Vous pouvez créer des niveaux avant approbation et après approbation. Pour obtenir des instructions sur la création d'un niveau d'approbation, reportez-vous à [Créer un niveau d'approbation](#).

Prérequis

Connectez-vous à la console vRealize Automation en tant qu'**administrateur de locataire** ou **administrateur d'approbation**.

Procédure

- 1 Sélectionnez **Administration > Stratégies d'approbation**.
- 2 Sélectionnez la ligne de la stratégie d'approbation à copier.
- 3 Cliquez sur l'icône **Copier** ().
Une copie de la stratégie est créée.
- 4 Sélectionnez la nouvelle stratégie d'approbation à modifier.
- 5 Entrez un nom dans la zone de texte **Nom**.
- 6 (Facultatif) Entrez une description dans la zone de texte **Description**.
- 7 Sélectionnez l'état de la stratégie dans le menu déroulant **Statut**.

Option	Description
Brouillon	Enregistre la stratégie d'approbation dans un état modifiable.
Actif	Enregistre la stratégie d'approbation dans un état de lecture seule que vous pouvez utiliser dans une autorisation.
Inactif	Enregistre la stratégie d'approbation dans un état de lecture seule que vous ne pouvez pas utiliser dans une autorisation avant d'avoir activé la stratégie.

- 8 Modifiez les niveaux avant approbation et après approbation.
- 9 Cliquez sur **OK**.

Vous avez créé une stratégie d'approbation à partir d'une stratégie existante.

Suivant

Appliquez la nouvelle stratégie à un droit d'accès. Reportez-vous à [Autoriser des utilisateurs à accéder à des services, des éléments de catalogue et des actions](#).

Désactiver une stratégie d'approbation

Lorsque vous considérez qu'une stratégie d'approbation est obsolète, vous pouvez la désactiver pour qu'elle ne soit plus disponible lors du provisionnement.

Pour désactiver une stratégie d'approbation, vous devez attribuer une nouvelle stratégie à chaque droit d'accès auquel la stratégie d'approbation est actuellement appliquée.

Vous pouvez par la suite réactiver une stratégie d'approbation désactivée ou la supprimer.

Prérequis

Connectez-vous à la console vRealize Automation en tant qu'**administrateur de locataire** ou **administrateur d'approbation**.

Procédure

- 1 Sélectionnez **Administration > Stratégies d'approbation**.
- 2 Cliquez sur le nom de la stratégie d'approbation.
- 3 Cliquez sur **Afficher les droits d'accès liés**.
 - a Dans le menu déroulant **Tout remplacer par**, sélectionnez la nouvelle stratégie d'approbation.
Si la liste inclut plusieurs autorisations, la nouvelle stratégie d'approbation s'applique à toutes les autorisations répertoriées.
 - b Cliquez sur **OK**.
- 4 Après avoir vérifié qu'aucun droit d'accès n'est lié à la stratégie d'approbation, sélectionnez **Inactif** dans le menu déroulant État.
- 5 Cliquez sur **OK**.
- 6 Pour supprimer une stratégie d'approbation, sélectionnez la ligne contenant la stratégie inactive.
 - a Cliquez sur **Supprimer**.
 - b Cliquez sur **OK**.

La stratégie d'approbation est dissociée de tout droit d'accès où elle utilisée et désactivée. Vous pouvez la réactiver ultérieurement et la réappliquer à des éléments dans un droit d'accès.

Suivant

Si vous n'avez plus besoin de la stratégie d'approbation, vous pouvez la supprimer. Reportez-vous à [Supprimer une stratégie d'approbation](#).

Supprimer une stratégie d'approbation

Si vous avez des stratégies d'approbation que vous avez désactivées et dont vous n'avez plus besoin, vous pouvez les supprimer depuis vRealize Automation.

Prérequis

- Dissociez et désactivez les stratégies d'approbation. Reportez-vous à [Désactiver une stratégie d'approbation](#).
- Connectez-vous à la console vRealize Automation en tant qu'**administrateur de locataire** ou **administrateur d'approbation**.

Procédure

- 1 Sélectionnez **Administration > Stratégies d'approbation**.
- 2 Sélectionnez la ligne contenant la stratégie inactive.
- 3 Cliquez sur **Supprimer**.
- 4 Cliquez sur **OK**.

La stratégie d'approbation est supprimée.

Scénario : créer et appliquer CentOS avec des stratégies d'approbation MySQL

En tant qu'administrateur de locataire pour le groupe d'activité de développement et d'ingénierie en qualité, vous voulez appliquer un contrôle strict aux demandes d'élément de catalogue. Avant que vos utilisateurs puissent provisionner le CentOS avec un élément de catalogue MySQL, vous voudrez que votre administrateur d'infrastructure virtuelle vSphere approuve la demande de machine et que votre gestionnaire de logiciel approuve la demande logicielle.

Vous créez et appliquez une stratégie d'approbation pour la machine CentOS vSphere avec une demande de service de catalogue MySQL pour que la machine nécessite une approbation de la part d'un administrateur d'infrastructure virtuelle vSphere sur la base de conditions spécifiques et une autre stratégie d'approbation pour que le composant Logiciel MySQL nécessite une approbation de la part de votre gestionnaire de logiciel pour chaque demande.

Les administrateurs d'approbation peuvent uniquement créer les approbations. Les gestionnaires de groupes d'activité peuvent ensuite les appliquer à des droits d'accès. En tant qu'administrateur de locataire, vous pouvez aussi bien créer les applications que les appliquer aux droits d'accès.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**. Seul un administrateur de locataire peut aussi bien créer qu'appliquer des stratégies d'approbation.
- Assurez-vous que l'élément de catalogue CentOS avec MySQL est inclus dans un service. Reportez-vous à [Scénario : mettre le Blueprint d'application CentOS avec MySQL à disposition dans le catalogue de services](#).

Scénario : créer une machine CentOS avec une stratégie d'approbation de machines virtuelles MySQL

En tant qu'administrateur de locataire, vous devez veiller à ce que le groupe d'ingénieurs qualité et développement reçoive des machines virtuelles correctement provisionnées dans votre environnement. Pour ce faire, créez une stratégie d'approbation qui requiert de pré-approuver certains types de demandes.


Étant donné que les machines virtuelles CentOS avec MySQL consomment des ressources vCenter Server, vous souhaitez que l'administrateur de l'infrastructure virtuelle vSphere approuve les demandes, lorsque la demande est supérieure à une mémoire de 2 048 Mo ou à deux CPU afin de garantir une utilisation cohérente des ressources. Par ailleurs, vous accordez à l'approbateur la capacité de modifier les valeurs demandées pour le CPU et la mémoire avant de procéder à l'approbation.

Procédure

- 1 Sélectionnez **Administration > Stratégies d'approbation**.
- 2 Créez une stratégie d'approbation pour le provisionnement de machine virtuelle.
 - a Cliquez sur l'icône **Nouveau** (+).
 - b Sélectionnez l'option **Sélectionnez un type de stratégie d'approbation**.
 - c Dans la liste, sélectionnez **Catalogue de services - Demande d'élément de catalogue - Machine virtuelle**.
 - d Cliquez sur **OK**.
 - e Configurez les options suivantes :

Option	Configuration
Nom	Entrez CPU ou mémoire de la machine virtuelle CentOS sur vSphere.
Description	Entrez Requiert l'approbation de l'admin IV pour CPU>2 ou mémoire>2048.
État	Sélectionnez l'option Actif .

- 3 Dans l'onglet **Pré-approbation**, cliquez sur l'icône **Ajouter** (+).
- 4 Configurez l'onglet **Informations sur le niveau** avec les critères de déclenchement et les actions d'approbation.
 - a Dans la zone de texte **Nom**, entrez **CPU>2 ou mémoire>2048 – Admin IV**.
 - b Dans la zone de texte **Description**, entrez
Approbation de l'admin IV pour le CPU et la mémoire.
 - c Sélectionnez **Requise en fonction des conditions**.
 - d Dans la liste déroulante **Clause**, sélectionnez **L'un des éléments suivants**.
 - e Dans la nouvelle liste déroulante **Clause**, sélectionnez **CPU** et configurez la clause avec les valeurs **CPU > 2**.
 - f Cliquez sur **Ajouter une expression** et configurez la clause avec les valeurs **Mémoire (Mo) > 2 048**.
 - g Sélectionnez **Utilisateurs et groupes spécifiques**.

- h Entrez le nom de l'administrateur de l'infrastructure virtuelle vSphere ou du groupe d'administrateurs dans la zone de recherche, puis cliquez sur l'icône de recherche (.
- i Sélectionnez l'utilisateur ou le groupe.
- j Sélectionnez **N'importe qui peut approuver**.

Un seul administrateur d'infrastructure virtuelle suffit pour vérifier les ressources et approuver la demande.

- 5 Cliquez sur l'onglet **Propriétés du système** et sélectionnez les propriétés qui permettent à l'approbateur de modifier, avant d'approuver une demande, les valeurs relatives au CPU et à la mémoire.
 - a Cochez les cases **CPU** et **Mémoire (Mo)**.
 - b Cliquez sur **OK**.
- 6 Cliquez sur **OK**.


Vous avez créé une stratégie d'approbation pour les demandes de machines virtuelles. Cependant, il vous reste à créer une approbation pour le composant MySQL. Aucune approbation n'est déclenchée tant que vous n'avez pas appliqué la stratégie à un droit d'accès.

Scénario : créer une stratégie d'approbation de composant Logiciel MySQL

En tant qu'administrateur de locataire, vos gestionnaires logiciels vous ont demandé de créer et d'appliquer des stratégies d'approbations pour que des installations MySQL puissent surveiller l'utilisation de licence. Vous créez une stratégie afin de notifier le gestionnaire de licence logicielle lorsque le composant Logiciel MySQL pour les machines virtuelles Linux est demandé.

Dans certains environnements, ce type d'approbation peut être nécessaire car les clés de licence doivent être fournies par le gestionnaire de logiciel. Dans ce scénario, le gestionnaire de logiciel n'a qu'à surveiller et approuver la demande. Une fois la stratégie d'approbation créée, vous appliquez la stratégie à l'élément de catalogue MySQL pour les machines virtuelles Linux. Cette stratégie d'approbation est très spécifique et peut uniquement être appliquée aux composants Logiciel MySQL pour machines virtuelles Linux dans les droits d'accès.

Procédure

- 1 Sélectionnez **Administration > Stratégies d'approbation**.
- 2 Créez une stratégie d'approbation pour le composant Logiciel MySQL.
 - a Cliquez sur l'icône **Nouveau** (.
 - b Sélectionnez **Sélectionner un élément**.
 - c Sélectionnez **MySQL pour machines virtuelles Linux**.

- d Cliquez sur **OK**.
- e Configurez les options suivantes :

Option	Configuration
Nom	Entrez approbation de suivi MySQL .
Description	Saisissez Demande d'approbation envoyée au gestionnaire de logiciel.
État	Sélectionnez l'option Actif .

- 3 Dans l'onglet **Pré-approbation**, cliquez sur l'icône **Ajouter** (+).
- 4 Configurez l'onglet **Informations sur le niveau** avec les critères de déclenchement et les actions d'approbation.
 - a Dans le champ de texte **Nom**, saisissez **notice de déploiement logiciel MySQL**.
 - b Dans le champ de texte **Description**, saisissez **Software mgr approbation d'installation logicielle**.
 - c Sélectionnez **Toujours requis**.
 - d Sélectionnez **Utilisateurs et groupes spécifiques**.
 - e Saisissez le nom du gestionnaire de logiciel dans la case de recherche et cliquez sur l'icône Rechercher (🔍), puis sélectionnez l'utilisateur.
 - f Sélectionnez **N'importe qui peut approuver**.
La demande ne nécessite l'approbation que d'un gestionnaire de logiciel.
Cliquez sur **OK**.

- 5 Cliquez sur **OK**.

Vous avez créé les stratégies d'approbation pour des machines virtuelles et pour MySQL à l'intention de composants Logiciel de machines virtuelles Linux. Aucune approbation n'est déclenchée tant que vous n'avez pas appliqué les stratégies d'approbation à un droit d'accès.

Scénario : application de stratégies d'approbation aux composants CentOS avec MySQL

En tant qu'administrateur de locataire, vous créez des stratégies et des droits d'approbation. Vous modifiez les droits de Dev et de QE à appliquer les stratégies d'approbation que vous avez créées afin que les approbations soient déclenchées quand un utilisateur du catalogue de services demande l'élément.

Bien qu'il soit peut-être plus facile d'autoriser l'accès à l'ensemble du service de catalogue à votre groupe d'activité, cela ne vous offre pas le même contrôle et la même gouvernance que la création d'autorisations individuelles pour des éléments de catalogue. Par exemple, si vous autorisez l'accès à un service à des utilisateurs, ils peuvent demander n'importe quel éléments de catalogue en service et tous les éléments ajoutés ultérieurement au service. Cela signifie aussi que vous pouvez seulement utiliser des stratégies d'approbation de haut niveau qui s'appliquent à chaque élément de catalogue, par exemple toujours demander l'approbation d'un gestionnaire. Si vous choisissez d'autoriser des éléments

de catalogue individuellement, vous pouvez créer et appliquer des stratégies d'approbation très spécifiques pour chaque élément et contrôler étroitement qui peut demander l'accès à quels éléments du service. Si vous choisissez d'autoriser l'accès à des composants spécifiques d'éléments de catalogue de manière individuelle, vous bénéficiez d'un contrôle encore plus grand.

Si vous n'êtes pas sûr des stratégies d'approbation à appliquer aux éléments dans un droit, vous pouvez y revenir ultérieurement pour les appliquer. Dans ce scénario, vous appliquez différentes stratégies d'approbation à deux composants du même Blueprint d'application publié.

Procédure

- 1 Sélectionnez **Administration > Gestion de catalogue > Droits d'accès**.
- 2 Cliquez sur le **Droit Dev et QE**.
- 3 Cliquez sur l'onglet **Éléments et approbations**.
- 4 Ajoutez la machine CentOS avec MySQL et appliquez la stratégie d'approbation.
 - a Cliquez sur l'icône **Ajouter des éléments (+)** en regard du titre **Éléments autorisés**.
 - b Cochez la case **CentOS avec MySQL**.
 - c Cliquez sur la flèche déroulante **Appliquer cette stratégie aux éléments sélectionnés**.
L'instance CentOS du CPU vSphere et de la stratégie de mémoire n'est pas dans la liste.
 - d Cliquez sur **Afficher tout**, puis sur la flèche déroulante pour afficher toutes les stratégies d'approbation.
 - e Sélectionnez **CentOS sur le CPU et la mémoire de vSphere [Catalogue de services - Demande d'élément de catalogue - Machine virtuelle]**.
La machine vSphere CentOS est un Blueprint de machine dans un Blueprint d'application. Passer en revue les noms de stratégie afin de sélectionner celui qui est approprié pour votre type d'élément de catalogue. Si vous appliquez la mauvaise stratégie, la stratégie d'approbation échoue ou déclenche des demandes d'approbation basées sur des conditions incorrectes.
 - f Cliquez sur **OK**.
- 5 Ajoutez le composant logiciel MySQL pour les machines virtuelles Linux en tant qu'élément et appliquez une stratégie d'approbation à l'élément MySQL.
 - a Cliquez sur l'icône **Ajouter des éléments et composants de catalogue (+)** en regard du titre **Éléments et composants de catalogue autorisés**.
 - b Dans le menu déroulant **Éléments et composants de catalogue**, sélectionnez **Non**.
Les composants logiciels sont toujours associés à une machine. Ils ne sont pas disponibles pour des demandes individuelles dans le catalogue de services.
 - c Cochez la case **MySQL pour les machines virtuelles Linux**.
 - d Cliquez sur la flèche déroulante **Appliquer cette stratégie aux éléments sélectionnés**.

- e Sélectionnez **approbation de suivi MySQL [Catalogue de services - Demande d'élément de catalogue - Composant logiciel]**.

Vous n'avez pas besoin de l'option avancée parce que la stratégie d'approbation avait été créée pour ce composant logiciel spécifique, qui est ajouté à une machine virtuelle.

- f Cliquez sur **OK**.

6 Ajoutez des actions que les utilisateurs peuvent exécuter sur la machine provisionnée.

Les stratégies d'approbation ne sont pas appliquées aux actions dans ce scénario.

- a Cliquez sur l'icône **Ajouter des actions** (+) en regard du titre Actions autorisées.
- b Sélectionnez les actions suivantes.

Nom/Type	Description
Créer un snapshot/une machine virtuelle	Crée un snapshot de machine virtuelle, y compris le logiciel installé. Permet aux développeurs de créer des snapshots auxquels ils peuvent revenir pendant le développement.
Détruire/Déploiement	Détruit le Blueprint entièrement provisionné, pas seulement la machine. Utilisez cette action pour éviter les composants orphelins.
Mettre hors tension/Machine	Met la machine virtuelle hors tension.
Mettre sous tension/Machine	Met la machine virtuelle sous tension.
Revenir au snapshot/Machine virtuelle	Revient au snapshot créé précédemment.

- c Cliquez sur **OK**.

7 Cliquez sur **Terminer**.

Ce droit vous autorise à demander différentes approbations concernant différents composants de Blueprint.

Suivant

Demandez l'élément CentOS avec MySQL dans le catalogue de services en tant que membre du groupe d'activité afin de vérifier que le droit et les approbations fonctionnent comme prévu.

Demander le provisionnement de machine à l'aide d'un Blueprint paramétré

Lorsque vous demandez le provisionnement de machine pour un Blueprint de machine vSphere qui a été conçu pour inclure les profils de composant de taille ou d'image, vous spécifiez le paramètre de provisionnement en sélectionnant un ensemble de valeurs disponible.

Lorsque vous demandez le provisionnement à partir du catalogue, vous pouvez sélectionner parmi les différents ensembles de valeurs disponibles pour les profils de composant Size et Image. Lorsque vous choisissez l'un des ensembles de valeurs, ses valeurs de propriété correspondantes sont ensuite liées à la demande.

L'ensemble de valeurs du profil de composant défini est appliqué à toutes les machines vSphere d'un cluster.

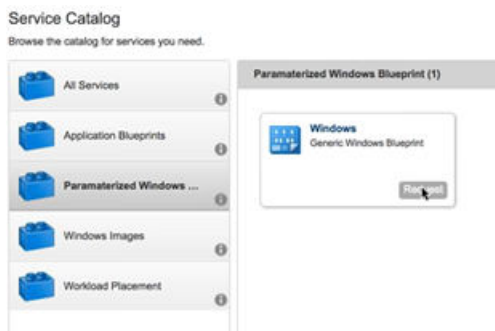
Pour plus d'informations sur la configuration du profil de composant, reportez-vous à la section [Présentation et utilisation du paramétrage de Blueprint](#).

Prérequis

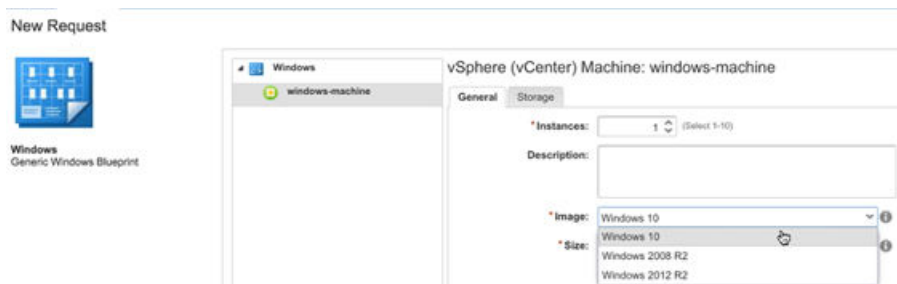
- Définissez des ensembles de valeurs pour les profils de composant Size ou Image. Consultez et dans *Référence des propriétés personnalisées*.
- Créez un Blueprint qui contient un composant de machine vSphere contenant un profil de composant Image ou Size. Reportez-vous à [Configurer un Blueprint de machine](#) et [Paramètres du composant de machine vSphere](#).
- Publiez le blueprint au catalogue. Reportez-vous à [Publier un Blueprint](#).
- Configurez le blueprint dans le catalogue. Reportez-vous à [Liste de contrôle pour la configuration du catalogue de services](#) et [Exemples de stratégies d'approbation basées sur le type de stratégie de machine virtuelle](#).

Procédure

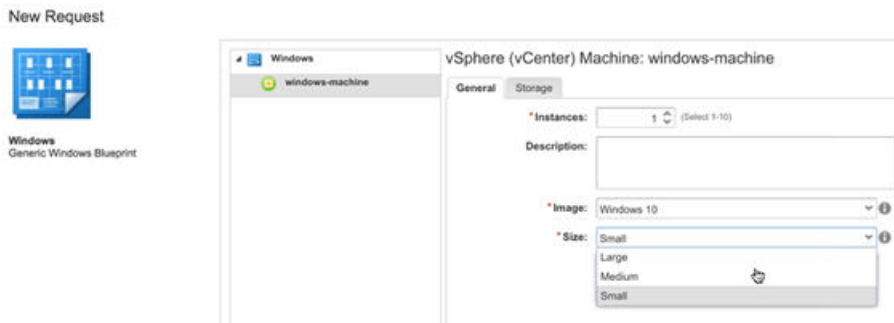
- 1 Cliquez sur **Catalogue**.
- 2 Sélectionnez le service de catalogue à demander et cliquez sur **Demander**.



- 3 Sélectionnez le composant de machine vSphere à provisionner et spécifiez le nombre d'instances à provisionner.
- 4 Sélectionnez une option d'ensemble de valeurs d'image dans le menu déroulant **Image**.



- 5 Sélectionnez une option d'ensemble de valeurs de taille dans le menu déroulant **Taille**.



- 6 Cliquez sur **Envoyer**.

Suivant

Les ensembles de valeurs que vous avez définis pour les profils de composant Size et Image sont désormais disponibles dans les menus déroulants **Image** et **Taille** de l'onglet **Catalogue** dans le formulaire de demande de provisionnement du catalogue.

Scénario : mettre le Blueprint d'application CentOS avec MySQL à disposition dans le catalogue de services

En tant qu'administrateur de locataire, vous avez demandé aux architectes du Blueprint de créer un élément du catalogue pour fournir MySQL sur des machines virtuelles CentOS, afin que le groupe d'ingénieurs qualité et développement puisse exécuter des cas de test. L'architecte de logiciels vous a informé que l'élément du catalogue est prêt à être mis à disposition des utilisateurs. Pour ce faire, associez les Blueprints et le composant Logiciel à un catalogue de services, puis autorisez les membres du groupe d'activité à demander l'élément.

Prérequis

- Connectez-vous à la console vRealize Automation en tant qu'**administrateur de locataire** ou **administrateur de catalogue**.
- Publiez un Blueprint pour livrer MySQL sur des machines virtuelles CentOS vSphere. Reportez-vous à *Installation et configuration de vRealize Automation pour le scénario Rainpole*.
- Si vous créez des Blueprints dans un environnement de développement, importez votre Blueprint dans votre environnement de production. Reportez-vous à [Exportation et importation de Blueprints et de contenu](#).
- Créez une réservation pour allouer des ressources vSphere au groupe d'activité d'ingénieurs qualité et développement. Reportez-vous à [Créer une réservation pour Hyper-V, KVM, SCVMM, vSphere ou XenServer](#).

Procédure

1 Scénario : créer un service de catalogue d'ingénierie de qualité et de développement

En tant qu'administrateur de locataire, vous voudrez créer un service de catalogue séparé pour votre groupe d'ingénierie de qualité et de développement de manière que vos autres groupes, par exemple celui des finances et des ressources humaines, n'aient pas accès aux éléments de catalogue spécialisés. Vous créez un service de catalogue appelé Service Dev et QE pour publier tous les éléments du catalogue que les personnes liées au développement et à l'ingénierie ont besoin pour procéder à leurs tests.

2 Scénario : ajouter CentOS avec MySQL au service Dev et QE

En tant qu'administrateur de locataire, vous souhaitez ajouter l'élément du catalogue CentOS avec MySQL au service Dev et QE.

3 Scénario : autoriser des utilisateurs à demander des éléments de service Dev et QE comme élément de catalogue

En tant qu'administrateur de locataire, vous créez une autorisation Dev et QE, et ajoutez les éléments de catalogue ainsi que quelques actions utiles afin que vos utilisateurs ingénieurs chargés du développement et de la qualité puissent demander l'élément de catalogue CentOS avec MySQL et exécuter des actions sur la machine et le déploiement.

Scénario : créer un service de catalogue d'ingénierie de qualité et de développement

En tant qu'administrateur de locataire, vous voudrez créer un service de catalogue séparé pour votre groupe d'ingénierie de qualité et de développement de manière que vos autres groupes, par exemple celui des finances et des ressources humaines, n'aient pas accès aux éléments de catalogue spécialisés. Vous créez un service de catalogue appelé Service Dev et QE pour publier tous les éléments du catalogue que les personnes liées au développement et à l'ingénierie ont besoin pour procéder à leurs tests.

Procédure

- 1 Sélectionnez **Administration > Gestion de catalogue > Services**.
- 2 Cliquez sur l'icône **Nouveau (+)**.
- 3 Saisissez le nom **Service Dev et QE** dans le champ de texte **Nom**.
- 4 Entrez la description **des éléments de catalogue d'application pour le développement et l'ingénierie** dans le champ de texte **Description**.
- 5 Sélectionnez **Actif** dans le menu déroulant **Statut**.
- 6 En tant qu'administrateur de catalogue créant le service, utilisez l'option de recherche pour ajouter votre nom comme propriétaire.

- 7 Ajoutez le groupe d'utilisateur personnalisé Équipe de support.

Par exemple, ajoutez un groupe d'utilisateur personnalisé qui comprend les architectes IaaS et les architectes de logiciel. Ainsi, les utilisateurs du catalogue de services et vous avez une personne à contacter si vous rencontrez des problèmes lors du provisionnement d'éléments du catalogue.

- 8 Cliquez sur **OK**.

Vous créez et activez un service de catalogue Dev et QE, mais il ne contient encore aucun élément de catalogue.

Scénario : ajouter CentOS avec MySQL au service Dev et QE

En tant qu'administrateur de locataire, vous souhaitez ajouter l'élément du catalogue CentOS avec MySQL au service Dev et QE.

Procédure

- 1 Sélectionnez **Administration > Gestion de catalogue > Services**.
- 2 Dans la liste **Services**, sélectionnez la ligne du service Dev et QE et cliquez sur **Gérer les éléments du catalogue**.
- 3 Cliquez sur l'icône **Nouveau (+)**.
- 4 Sélectionnez **CentOS avec MySQL**.

Seuls les Blueprints publiés et les composants pas encore associés à un service sont affichés dans la liste. Si le Blueprint n'apparaît pas, vérifiez qu'il a été publié ou qu'il n'est pas inclus dans un autre service.
- 5 Cliquez sur **OK**.
- 6 Cliquez sur **Fermer**.

Vous avez publié l'élément du catalogue CentOS avec MySQL à destination du service Dev et QE. Cependant, personne ne peut voir l'élément ni le demander tant que n'avez pas accordé aux utilisateurs des droits d'accès à l'élément ou au service.

Scénario : autoriser des utilisateurs à demander des éléments de service Dev et QE comme élément de catalogue

En tant qu'administrateur de locataire, vous créez une autorisation Dev et QE, et ajoutez les éléments de catalogue ainsi que quelques actions utiles afin que vos utilisateurs ingénieurs chargés du développement et de la qualité puissent demander l'élément de catalogue CentOS avec MySQL et exécuter des actions sur la machine et le déploiement.

Dans ce scénario, vous autorisez le service, car vous souhaitez que les utilisateurs aient accès à tout futur élément de catalogue ajouté à ce service. Vous voulez aussi autoriser les utilisateurs à gérer leur déploiement provisionné. Pour cela, ajoutez des actions tels que démarrage et arrêt, snapshot et destruction du déploiement à l'autorisation.

Procédure

- 1 Sélectionnez **Administration > Gestion de catalogue > Droits d'accès**.
- 2 Cliquez sur l'icône **Nouveau (+)**.
- 3 Configurez les détails.
 - a Saisissez le nom **Autorisation Dev et QE** dans le champ de texte **Nom**.
 - b Dans le menu déroulant **État**, sélectionnez **Actif**.
 - c Dans le menu déroulant **Groupe d'activité**, sélectionnez le groupe **Dev et QE**.
 - d Dans la zone Utilisateurs et groupes, ajoutez un ou plusieurs utilisateurs.

Ajoutez-vous uniquement, sauf si vous êtes sûr que le Blueprint fonctionne comme désiré. Si c'est le cas, vous pouvez ajouter des utilisateurs individuels et des groupes d'utilisateurs personnalisés.

- e Cliquez sur **Suivant**.
- 4 Ajoutez le service.

Bien que vous ajoutiez les éléments de catalogue CentOS et MySQL séparément, l'ajout du service garantit que tout élément supplémentaire ajouté au service à une date ultérieure est disponible pour les membres du groupe d'activité dans le catalogue de service.

- a Cliquez sur l'icône **Ajouter des services (+)** en regard du titre Services autorisés.
 - b Sélectionnez **Service Dev et QE**.
 - c Cliquez sur **OK**.

Le service Dev et QE est ajouté à la liste des services autorisés.

5 Ajoutez des actions.

- a Cliquez sur l'icône **Ajouter des actions** (+) en regard du titre Actions autorisées.
- b Cliquez sur l'en-tête de la colonne Type pour trier la liste.

Sélectionnez les actions suivantes en fonction du type : Ces actions sont utiles pour les utilisateurs ingénieurs en développement et en qualité qui travaillent avec leurs machines de test. Il s'agit des seules actions que vous voulez que les membres de ce groupe d'activité utilisent.

Type	Nom d'action
Machine	Mettre sous tension
Machine	Mettre hors tension
Machine virtuelle	Créer un instantané
Machine virtuelle	Revenir au snapshot
Déploiement	Détruire L'action de destruction du déploiement détruit l'ensemble du déploiement et pas seulement la machine virtuelle.

- c Cliquez sur **OK**.

Les cinq actions sont ajoutées à la liste d'actions autorisées.

6 Cliquez sur **Terminer**.

Vous avez ajouté l'élément de catalogue CentOS avec MySQL à votre nouveau service de catalogue Dev et QE, et autorisé les membres de votre groupe d'activité à faire appel à l'élément et à le gérer.

Suivant

Après avoir vérifié votre travail en provisionnant l'élément de catalogue CentOS avec MySQL, vous pouvez ajouter des utilisateurs supplémentaires pour rendre l'élément de catalogue disponible publiquement à vos utilisateurs ingénieurs chargés du développement et de la qualité. Si vous souhaitez gérer plus en détail le provisionnement des ressources dans votre environnement, vous pouvez créer des stratégies d'approbation pour le composant MySQL Logiciel et la machine CentOS de test logiciel. Reportez-vous à [Scénario : créer et appliquer CentOS avec des stratégies d'approbation MySQL](#).

Gestion des éléments de catalogue déployés

Vous pouvez afficher et prendre des mesures sur les déploiements provisionnés, y compris les machines, les équilibres de charge, les réseaux et les autres ressources de déploiement.

Exécution d'actions pour des ressources provisionnées

Les actions disponibles pour une ressource provisionnée varient selon le type de ressource, la méthode de configuration et de mise à disposition de l'action pour les éléments provisionnés et l'état opérationnel de l'élément.

Les actions configurées qui sont disponibles pour une machine ou un déploiement provisionné s'affichent dans le menu **Actions** pour la ressource sélectionnée dans l'onglet **Éléments**.

Si l'élément a été provisionné par IaaS au moyen d'un Blueprint de machine IaaS, la liste des actions disponibles est déterminée en fonction des éléments sélectionnés dans l'onglet **Actions** pour le composant du type de machine lors de la création du Blueprint, puis selon les éléments applicables selon le type ou l'état de la machine.

Si l'élément a été provisionné au moyen d'un Blueprint XaaS, les actions de ressource doivent être créées, publiées et rendues accessibles dans le même service que celui utilisé pour provisionner l'élément. La liste des actions disponibles est déterminée par le type d'élément et l'état actuel de l'élément.

Les actions disponibles pour un élément qui a été provisionné en tant que machine IaaS peut aussi inclure des actions de ressource XaaS si les actions sont mappées à l'élément.

Commandes du menu Action pour les ressources provisionnées

Les actions sont des modifications que vous pouvez apporter aux ressources provisionnées. Les actions vRealize Automation sont utilisées pour gérer le cycle de vie des ressources.

Les commandes du menu **Action** pour une ressource provisionnée incluent les actions spécifiées dans le plan et peuvent également inclure des opérations de menu personnalisées créées par vos architectes de services. Les actions disponibles varient selon la manière dont votre gestionnaire de groupe d'activité ou votre administrateur de locataire a configuré le droit contenant la ressource sur laquelle les actions sont exécutées.

Vous ne devez pas gérer les objets NSX administrés par vRealize Automation en dehors de vRealize Automation. Par exemple, si vous modifiez le port membre d'un équilibrage de charge NSX déployé dans NSX, plutôt que dans vRealize Automation, la collecte de données NSX rompt l'association entre la machine déployée et son pool de membres de l'équilibrage de charge associé ailleurs. Les opérations de réduction de charge et de montée en charge génèrent également des résultats inattendus si un port membre de l'équilibrage de charge déployé est modifié à l'extérieur de vRealize Automation.

Tableau 3-75. Commandes du menu Action

Action	Type de ressource	Description
Associer une adresse IP flottante	Machine (OpenStack)	Associer une adresse IP flottante à une machine OpenStack.
Annuler la reconfiguration	Machine	Annulez une action de reconfiguration en cours d'exécution.
Modifier le bail	Déploiement et machine	Modifiez le nombre de jours restant dans le bail pour une machine spécifique ou pour toutes les ressources incluses dans un déploiement. Si vous ne fournissez pas de valeur, le bail n'expire pas.

Tableau 3-75. Commandes du menu Action (suite)

Action	Type de ressource	Description
Changer le propriétaire	Déploiement	<p>Modifiez le propriétaire du déploiement et de toutes les ressources incluses. Seuls les gestionnaires de groupes d'activité et les utilisateurs de support technique peuvent modifier la propriété d'un déploiement.</p> <p>La machine doit être dans l'état sous tension, hors tension ou actif lorsque vous lancez l'action de changement de propriétaire, sinon l'action échoue et le message suivant s'affiche :</p> <p>L'action n'est pas valide pour la machine.</p>
Se connecter à l'aide de VMRC	Machine	<p>Connectez-vous à la machine virtuelle à l'aide d'une application VMRC 8.x.</p> <p>Pour utiliser cette action, l'application VMRC doit être installée sur le système local de l'utilisateur du catalogue de services qui exécute l'action.</p> <p>Pour l'installation et les instructions utilisateur, reportez-vous à Documentation VMware Remote Console. Pour le téléchargement, reportez-vous à Télécharger VMware Remote Console.</p> <p>VMRC 8.x remplace VMware Remote Console utilisé précédemment.</p>
Se connecter à la console distante	Machine	<p>Connectez-vous à la machine sélectionnée à l'aide de VMware Remote Console.</p> <p>La console de la machine virtuelle s'affiche dans le navigateur.</p> <p>VMRC 8.x remplace VMware Remote Console.</p>
Se connecter à l'aide du ticket de console	Machine (OpenStack et KVM)	<p>Connectez-vous à la machine virtuelle OpenStack ou KVM au moyen d'un ticket de console pour une connexion VMware Remote Console.</p>
Se connecter via ICA	Machine (Citrix)	<p>Connecter-vous à la machine Citrix via Independent Computing Architecture.</p>

Tableau 3-75. Commandes du menu Action (suite)

Action	Type de ressource	Description
Se connecter via RDP	Machine	Connectez-vous à la machine via Microsoft Remote Desktop Protocol.
Se connecter via SSH	Machine	<p>Se connecte à la machine sélectionnée via SSH.</p> <p>L'option Se connecter via SSH nécessite que votre navigateur dispose d'un plug-in prenant en charge SSH, par exemple le client de terminal SSH FireSSH pour Mozilla Firefox et Google Chrome. Lorsque le plug-in est présent, la sélection de l'option Se connecter via SSH affiche une console SSH et vous invite à entrer vos informations d'identification d'administrateur.</p> <p>Pour utiliser cette action, la propriété personnalisée Machine. SSH doit être incluse et définie sur True dans le composant de machine du Blueprint, soit dans un groupe de propriétés, soit dans un groupe personnalisé individuel.</p>
Se connecter via Virtual Desktop	Machine	Connectez-vous à la machine sélectionnée via Microsoft Virtual Desktop.
Créer un snapshot	Machine virtuelle	Créez un snapshot de la machine virtuelle. Si vous avez droit à seulement deux snapshots et que vous en disposez déjà, cette commande n'est pas disponible tant que vous n'en supprimez pas un.
Supprimer le snapshot	Machine virtuelle	Supprimez un snapshot de la machine virtuelle.

Tableau 3-75. Commandes du menu Action (suite)

Action	Type de ressource	Description
Détruire	Machine cloud, déploiement, machine virtuelle et NSX Edge	<p>Détruisez immédiatement une ressource provisionnée. Vous devez exécuter cette action pour détruire les ressources XaaS, même si elles font partie d'un déploiement que vous détruisez. Les autres ressources sont détruites à la fin de leur bail ou de leur période d'archivage.</p> <p>À l'exception de XaaS, la destruction des composants d'un déploiement n'est pas recommandée. Utilisez l'action de réduction de charge pour réduire le nombre de machines dans votre déploiement ou détruisez l'intégralité du déploiement.</p> <p>L'action Détruire n'est pas disponible pour les situations de déploiement suivantes :</p> <ul style="list-style-type: none"> ■ déploiements de machine physique ■ déploiements avec un réseau NSX existant ou une ressource de sécurité NSX existante ■ déploiements avec une ressource d'équilibrage de charge à la demande NSX <p>Puisqu'un équilibrage de charge NSX est la propriété d'un dispositif NSX Edge à la demande, lorsque le dispositif NSX Edge est détruit, la ressource d'équilibrage de charge l'est également et les ressources sont libérées.</p> <p>Lorsqu'un niveau de machine dont la charge est équilibrée est détruit, il est supprimé du pool d'équilibrage de charge sur l'Edge NSX en question.</p> <p>Les administrateurs de groupes d'activité peuvent choisir de forcer la destruction d'un déploiement après l'échec d'une demande de destruction. La destruction forcée indique à vRealize Automation d'ignorer les échecs de destruction des ressources individuelles en détruisant le déploiement. Pour</p>

Tableau 3-75. Commandes du menu Action (suite)

Action	Type de ressource	Description
		<p>plus d'informations sur l'utilisation de la destruction forcée, reportez-vous à la section Forcer la destruction d'un déploiement après l'échec d'une demande de destruction.</p> <hr/> <p>Remarque Le stockage et la mémoire alloués à une machine provisionnée via une réservation sont libérés lorsque la machine est supprimée dans vRealize Automation par l'action Détruire. Le stockage et la mémoire ne sont pas libérés si la machine est supprimée dans vCenter Server.</p> <hr/> <p>Lors de la destruction d'un déploiement contenant un composant de machine Amazon, tous les volumes EBS ajoutés à la machine pendant son cycle de vie sont détachés plutôt que détruits. vRealize Automation ne propose pas d'option permettant de détruire les volumes EBS.</p>
Détruire un réseau existant	Réseau existant	Détruisez le réseau.
Détruire un équilibrage de charge VMware NSX	Équilibrage de charge VMware NSX	Détruisez l'équilibrage de charge NSX.
Détruire un réseau VMware NSX	Réseau VMware NSX	Détruisez le réseau NSX.
Détruire un groupe de sécurité VMware NSX	Groupe de sécurité VMware NSX	Détruisez le groupe de sécurité VMware NSX.
Détruire une balise de sécurité VMware NSX	Balise de sécurité VMware NSX	Détruisez la balise de sécurité NSX.
Dissocier les adresses IP flottantes	Machine (OpenStack)	Supprimez l'adresse IP flottante de la machine OpenStack.
Exécuter la reconfiguration	Machine	Remplacez une reconfiguration planifiée, ou relancez ou replanifiez une reconfiguration ayant échoué.
Date d'expiration	Déploiement et machine	Terminez le déploiement ou le bail de machine pour toutes les ressources incluses dans le déploiement.
Exporter le certificat	Machine	Exportez le certificat d'une machine cloud.

Tableau 3-75. Commandes du menu Action (suite)

Action	Type de ressource	Description
Obtenir un rappel d'expiration	Machine	Télécharge un fichier d'événement de calendrier pour la date d'expiration de bail actuelle.
Installer VMware Tools	Machine	Installez VMware Tools sur une machine virtuelle vSphere.
Cycle d'alimentation	Machine	Met la machine hors tension, puis la remet sous tension.
Mettre hors tension	Machine	Met la machine hors tension sans arrêter le système d'exploitation invité.
Mettre sous tension	Machine	Mettez la machine sous tension. Si la machine a été interrompue, le fonctionnement normal reprend à partir du moment où la machine a été interrompue.
Redémarrage	Machine	Redémarrez le système d'exploitation invité sur une machine virtuelle vSphere. VMware Tools doit être installé sur la machine pour utiliser cette action.

Tableau 3-75. Commandes du menu Action (suite)

Action	Type de ressource	Description
Reconfigurer	Machine	<p>Un gestionnaire de groupes d'activité, un utilisateur de support technique ou le propriétaire d'une machine peut effectuer les actions suivantes de reconfiguration de la machine vSphere sélectionnée :</p> <ul style="list-style-type: none"> ■ Modifier la description ■ Modifier les paramètres de CPU, de mémoire, de réseau et de disque ■ Ajouter, modifier et supprimer des propriétés personnalisées et des groupes de propriétés ■ Ajouter, modifier ou supprimer des balises de sécurité et des groupes de sécurité ■ Ajouter, modifier, réorganiser ou supprimer des règles de réacheminement de port NAT ■ Reconfigurer l'arrêt ■ Modifier le propriétaire de la machine (disponible uniquement pour les gestionnaires de groupes d'activité et les utilisateurs de support technique) <p>Vous ne pouvez pas modifier une stratégie de réservation de stockage si une telle intervention modifie le profil de stockage sur un disque.</p>
Reconfigurer	Équilibrage de charge	<p>Un propriétaire de machine autorisé, un utilisateur d'assistance, un administrateur de locataire ou un gestionnaire de groupes d'activité peut modifier les paramètres dans un serveur virtuel et peut ajouter ou supprimer des serveurs virtuels dans l'équilibrage de charge NSX :</p> <p>Pour plus d'informations sur les paramètres de serveur virtuel dans l'équilibrage de charge, reportez-vous à la section Ajouter un composant d'équilibrage de charge à la demande.</p>
Enregistrer VDI	Machine virtuelle (XenServer)	Enregistrez l'image de disque virtuel dans des éléments XenServer.

Tableau 3-75. Commandes du menu Action (suite)

Action	Type de ressource	Description
Reprovisionner	Machine	<p>Détruit la machine, puis démarre le workflow de provisionnement pour créer une machine portant le même nom.</p> <p>Lorsque vous demandez le provisionnement d'une machine, un problème connu peut entraîner vRealize Automation à afficher l'état du reprovisionnement dans le catalogue comme étant Terminé, alors que son état réel est En cours. Après avoir soumis une demande de reprovisionnement d'une machine, vous pouvez utiliser n'importe laquelle des séquences suivantes pour vérifier l'état de la machine reprovisionné :</p> <ul style="list-style-type: none"> ■ Infrastructure > Machines gérées ■ Éléments > Détails de l'élément ■ Administration > Événements > Journaux des événements <p>Remarque Vous ne pouvez pas reprovisionner une machine Amazon.</p> <p>Pour plus d'informations, voir l'article de la base de connaissances VMware Reprovisioned machine tasks... (2065873) à l'adresse http://kb.vmware.com/kb/2065873.</p>
Restaurer le snapshot	Machine virtuelle	<p>Restaurer un snapshot de cette machine. Vous devez disposer d'un snapshot existant pour utiliser cette action.</p>

Tableau 3-75. Commandes du menu Action (suite)

Action	Type de ressource	Description
Réduire la charge	Déploiement	<p>Détruisez les instances inutiles des machines dans votre déploiement pour ajuster le système à des besoins de capacité réduits. Les composants de machines et les composants logiciels qui y sont installés sont détruits. Les composants logiciels dépendants, ainsi que les composants de mise en réseau et de sécurité sont mis à jour pour la nouvelle configuration de déploiement. Les composants XaaS ne sont pas évolutifs et ne sont pas mis à jour lors des opérations de dimensionnement. Vous pouvez essayer de réparer les opérations de dimensionnement partiellement réussies en tentant de redimensionner le déploiement. Il n'est cependant pas possible de dimensionner un déploiement à sa taille actuelle. En outre, le fait de réparer un dimensionnement partiellement réussi de cette manière ne permet pas de désallouer les ressources non résolues. Vous pouvez accéder à l'écran de détail de l'exécution de la demande et rechercher les tâches qui ont échouées, ainsi que les nœuds concernés, pour déterminer s'il est judicieux de réparer le dimensionnement partiellement réussi à l'aide d'une autre opération de dimensionnement. Les opérations de dimensionnement partiellement réussies et ayant échoué n'ont pas d'incidence sur la fonctionnalité de votre déploiement initial et vous pouvez continuer à utiliser vos éléments de catalogue lors de la résolution des erreurs.</p>

Tableau 3-75. Commandes du menu Action (suite)

Action	Type de ressource	Description
Monter en charge	Déploiement	<p>Provisionnez des instances supplémentaires de machines dans votre déploiement pour l'ajuster à vos besoins en matière d'accroissement des capacités. Les composants de machines et les composants logiciels qui y sont installés sont provisionnés. Les composants logiciels dépendants, ainsi que les composants de mise en réseau et de sécurité sont mis à jour pour la nouvelle configuration de déploiement. Les composants XaaS ne sont pas évolutifs et ne sont pas mis à jour lors des opérations de dimensionnement.</p> <p>Vous pouvez essayer de réparer les opérations de dimensionnement partiellement réussies en tentant de redimensionner le déploiement. Il n'est cependant pas possible de dimensionner un déploiement à sa taille actuelle. En outre, le fait de réparer un dimensionnement partiellement réussi de cette manière ne permet pas de désallouer les ressources non résolues. Vous pouvez accéder à l'écran de détail de l'exécution de la demande et rechercher les tâches qui ont échouées, ainsi que les nœuds concernés, pour déterminer s'il est judicieux de réparer le dimensionnement partiellement réussi à l'aide d'une autre opération de dimensionnement. Les opérations de dimensionnement partiellement réussies et ayant échoué n'ont pas d'incidence sur la fonctionnalité de votre déploiement initial et vous pouvez continuer à utiliser vos éléments de catalogue lors de la résolution des erreurs.</p>
Arrêt	Machine	<p>Arrête le système d'exploitation invité et met la machine virtuelle hors tension. VMware Tools doit être installé sur la machine pour utiliser cette action.</p>

Tableau 3-75. Commandes du menu Action (suite)

Action	Type de ressource	Description
Interrompre	Machine	Mettez la machine en pause de sorte qu'elle ne puisse pas être utilisée et qu'elle ne consomme aucune ressource système autre que le stockage qu'elle utilise.
Annuler l'inscription	Machine	Retirez la machine de l'inventaire sans la détruire. Les machines non enregistrées ne sont pas utilisables.
Annuler l'inscription de VDI	Machine virtuelle (XenServer)	Annulez l'inscription de l'image de disque virtuel sur les éléments XenServer.

Configurer un fournisseur de mesures

Vous pouvez configurer vRealize Automation pour utiliser les mesures de santé et de ressources de vRealize Operations Manager pour les machines virtuelles vSphere.

Pour plus d'informations sur les badges et mesures de santé de vRealize Operations Manager, consultez la documentation de vRealize Operations Manager.

Prérequis

- Connectez-vous à la console vRealize Automation en tant qu'**administrateur de locataire**, **gestionnaire de groupes d'activité** ou **propriétaire de machine**.
- Créez un compte d'utilisateur vRealize Operations Manager user disposant de privilèges d'affichage et de requête de mesures de ressources pour tous les serveurs vSphere que vous intégrez à vRealize Automation.
- Créez des instances d'adaptateur vRealize Operations Manager pour tous les serveurs vSphere que vous ajoutez en tant que points de terminaison dans vRealize Automation. Pour plus d'informations sur la création d'instances d'adaptateur, consultez la documentation de vRealize Operations Manager.

Procédure

- 1 Sélectionnez **Administration > Récupération > Fournisseur de mesures**.
- 2 Sélectionnez un fournisseur de mesures.

Option	Description
Fournisseur de mesures vRealize Automation par défaut	Si vous n'avez pas d'instance de vRealize Operations Manager, vRealize Automation fournit les mesures de machines de base.
Point de terminaison vRealize Operations Manager	Fournissez des informations de connexion pour l'instance de vRealize Operations Manager que vous souhaitez utiliser comme votre fournisseur de mesures pour les machines virtuelles vSphere.

3 Cliquez sur **Tester la connexion**.

4 Cliquez sur **Enregistrer**.

Les administrateurs de locataire, les propriétaires de machines et les gestionnaires de groupes d'activité du groupe dans lequel réside la machine peuvent afficher des badges de santé et des alertes de santé sur les pages de détails d'éléments des machines virtuelles vSphere. Ils peuvent également afficher des mesures et des badges de santé de vRealize Operations Manager lorsqu'ils filtrent par type de plateforme vSphere sur la page des récupérations.

Suivant

[Envoyer des demandes de récupération](#).

Envoyer des demandes de récupération

Vous pouvez afficher et gérer les déploiements et envoyer des demandes de récupération aux propriétaires des déploiements. Une demande de récupération spécifie une nouvelle durée de bail en jours, la durée accordée au propriétaire d'un déploiement pour répondre et quelles machines cibler lors de la récupération.

Prérequis

- Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.
- (Facultatif) Pour afficher des badges d'état de santé ou des mesures fournies par vRealize Operations Manager, reportez-vous à la section [Configurer un fournisseur de mesures](#).

Procédure

1 Sélectionnez **Administration > Récupération > Déploiements**.

2 Recherchez les déploiements de machine virtuelle correspondant à vos critères de recherche.

Vous devez sélectionner le type de plate-forme vSphere pour afficher les mesures fournies par vRealize Operations Manager.

- a Cliquez sur la flèche vers le bas **Recherche avancée** pour ouvrir la zone de recherche.
- b Entrez ou sélectionnez une ou plusieurs valeurs de recherche.

Option	Action
Le nom de la machine virtuelle contient	Entrez un ou plusieurs caractères dans la zone de texte pour rechercher des noms de machines virtuelles correspondants.
Le nom du propriétaire contient	Entrez un nom dans la zone de texte pour rechercher des noms de propriétaires correspondants.
Les noms des groupes d'activité contiennent	Entrez un nom dans la zone de texte pour rechercher des noms de groupes d'activité correspondants.
Type de plate-forme	Sélectionnez un type de plate-forme dans le menu déroulant. Sélectionnez vSphere pour afficher les mesures fournies par vRealize Operations Manager. Requis pour vRealize Operations Manager.
État de l'alimentation	Sélectionnez une valeur d'état de l'alimentation dans le menu déroulant pour rechercher des machines virtuelles avec un état d'alimentation correspondant.
Date d'expiration comprise entre	Cliquez sur les icônes de calendrier et sélectionnez des dates de début et de fin pour rechercher des dates d'expiration situées dans la plage.
Utilisation du CPU	Sélectionnez une valeur dans le menu déroulant pour rechercher des machines virtuelles avec une utilisation de CPU élevée, supérieure à 80 %, une utilisation de CPU inférieure à 5 % ou Aucune, pour aucune valeur. Si vous faites une demande de mesures vRealize Operations Manager, vous ne pouvez pas utiliser ce filtre pour la demande, ni trier les résultats en fonction de l'utilisation du CPU.
Utilisation de la mémoire	Sélectionnez une valeur dans le menu déroulant pour rechercher des machines virtuelles avec une utilisation de mémoire élevée, supérieure à 80 %, une utilisation de mémoire inférieure à 10% ou Aucune, pour aucune valeur. Si vous faites une demande de mesures vRealize Operations Manager, vous ne pouvez pas utiliser ce filtre pour la demande, ni trier les résultats en fonction de l'utilisation de la mémoire.
Utilisation du disque	Sélectionnez une valeur dans la liste déroulante pour rechercher des machines virtuelles avec une utilisation de disque dur faible, inférieure à 2 Ko par seconde ou Aucune, pour aucune valeur. Si vous faites une demande de mesures vRealize Operations Manager, vous ne pouvez pas utiliser ce filtre pour la demande, ni trier les résultats en fonction de l'utilisation du disque.

Option	Action
Utilisation du réseau	<p>Sélectionnez une valeur dans la liste déroulante pour rechercher des machines virtuelles avec une utilisation de réseau faible, inférieure à 1 Ko par seconde ou Aucune, pour aucune valeur.</p> <p>Si vous faites une demande de mesures vRealize Operations Manager, vous ne pouvez pas utiliser ce filtre pour la demande, ni trier les résultats en fonction de l'utilisation du réseau.</p>
Mesure complexe	<p>Sélectionnez une valeur dans le menu déroulant pour rechercher des machines virtuelles en fonction de mesures complexes. Par exemple, sélectionnez « inactif » pour rechercher des machines dont les valeurs d'utilisation de CPU, de réseau, de mémoire et de disque sont toutes inférieures à 20 %.</p> <p>Vous ne pouvez pas utiliser ce filtre si vous faites une demande de mesures vRealize Operations Manager.</p>

^c Cliquez sur l'icône de recherche (🔍).

- 3 Sur la page Déploiements, sélectionnez une ou plusieurs machines dont le déploiement parent doit être récupéré.

Seules les machines sélectionnées qui apparaissent sur la page des résultats courante sont récupérées.

- 4 Cliquez sur **Récupération**.

Les déploiements contenant des machines virtuelles qui sont sélectionnés sur la page courante sont inclus dans la demande.

Remarque La page Déploiement de récupération peut répertorier des machines ne pouvant pas être récupérées, comme les machines dont le bail a expiré. Si vous spécifiez une machine ne pouvant pas être récupérée, l'erreur suivante s'affiche :

```
Selection Error: Virtual machine name is not in valid state for reclamation.
```

- 5 Entrez la durée du nouveau bail dans la zone de texte **Durée du nouveau bail (jours)**.

La durée minimale est de 1 jour, la durée maximale est de 365 jours et la valeur par défaut est 7 jours.

- 6 Entrez le nombre de jours accordés au propriétaire du déploiement pour répondre à la demande de récupération dans la zone de texte **Attente avant d'imposer le bail (jours)**.

À la fin de ce délai, le déploiement reçoit un nouveau bail avec une nouvelle durée de bail. La durée d'attente minimale est de 1 jour, la durée maximale est de 365 jours et la valeur par défaut est 3 jours.

- 7 Entrez un motif pour la demande dans la zone de texte **Motif de la demande**.

- 8 Cliquez sur **Envoyer**.

- 9 Cliquez sur **OK**.

Lorsque vous envoyez une demande de récupération, elle apparaît dans la boîte de réception du propriétaire du déploiement. Si le propriétaire ne répond pas à la demande pendant la période qui lui est accordée, le déploiement reçoit un nouveau bail de la durée spécifiée, sauf si la durée de son bail actuel est plus courte. Si le propriétaire clique sur **Élément en cours d'utilisation** sur la demande de récupération, le bail du déploiement reste inchangé. Si le propriétaire clique sur **Libérer pour récupération**, le bail du déploiement expire immédiatement.

Suivant

[Suivi des demandes de récupération.](#)

Suivi des demandes de récupération

Vous pouvez effectuer le suivi de l'état actuel des demandes de récupération et autres détails.

Les autres méthodes suivantes sont disponibles pour vérifier une demande de récupération récente :

- Cliquer sur l'onglet **Boîte de réception** et sélectionner **Demandes de récupération** pour afficher les informations sur les demandes de récupération.
- Cliquer sur l'onglet **Demandes de récupération** et afficher la liste des demandes récentes.
- Cliquez sur l'onglet **Éléments** et sélectionner **Déploiements** pour afficher les modifications apportées aux déploiements.


Prérequis

Connectez-vous à la console de vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

- 1 Sélectionnez **Administration > Récupération > Demandes de récupération**.
- 2 Recherchez les machines virtuelles correspondant à vos critères de recherche.
 - a Cliquez sur la flèche vers le bas **Recherche avancée** pour ouvrir la zone de recherche.
 - b Tapez ou sélectionnez une ou plusieurs valeurs de recherche.

Option	Action
Le nom de la machine virtuelle contient	Tapez un ou plusieurs caractères dans la zone de texte pour rechercher des noms de machines virtuelles correspondants.
Le nom du propriétaire contient	Tapez un ou plusieurs caractères dans la zone de texte pour rechercher des noms de propriétaires correspondants.
Le motif de la demande contient	Tapez un ou plusieurs caractères dans la zone de texte pour rechercher un motif de demande correspondant.
État de la demande	Sélectionnez une valeur d'état de demande dans le menu déroulant pour rechercher des machines virtuelles avec un état de demande correspondant.

- c Cliquez sur l'icône **Rechercher** () ou appuyez sur Entrée pour démarrer la recherche.
- d Cliquez sur la flèche vers le haut **Recherche avancée** pour fermer la zone de recherche.

- 3 (Facultatif) Cliquez sur **Actualiser les données** pour mettre à jour l'affichage des demandes de récupération.

Modifier la réservation d'une machine gérée

Vous pouvez modifier le paramètre de réservation ou de stockage d'une machine gérée. Cette possibilité est utile lorsqu'une machine est déplacée vers un nouveau chemin de stockage qui n'est pas disponible dans la réservation sa réservation actuelle. Pour le déploiement sur une seule machine, vous pouvez également modifier le groupe d'activité de la machine.

Vous pouvez déplacer une machine, dans le cas d'un déploiement sur une seule machine, vers un autre groupe d'activité si le propriétaire de la machine est membre du groupe d'activité cible. Vous devez être un gestionnaire de groupe d'activité des groupes d'origine et cible pour modifier le paramètre d'un groupe d'activité.

Remarque Si une stratégie de réservation est affectée à la machine, vous ne pouvez pas modifier son groupe d'activité.

Vous pouvez créer des réservations supplémentaires pour la ressource de calcul associée en utilisant les options de menu **Administration > Ressources de calcul**.

Le stockage et la mémoire alloués à une machine provisionnée via une réservation sont libérés lorsque la machine est supprimée dans vRealize Automation par l'action Détruire. Le stockage et la mémoire ne sont pas libérés si la machine est supprimée dans vCenter Server.

Par exemple, vous ne pouvez pas supprimer une réservation associée aux machines d'un déploiement existant. Si vous déplacez ou supprimez des machines déployées manuellement dans vCenter Server, vRealize Automation continue de reconnaître les machines déployées comme étant en temps réel et vous empêche de supprimer les réservations associées.

Si la modification de la réservation déplace une machine dans vCenter Server vers un nouveau chemin de stockage qui ne fait pas partie de cette réservation de machine dans vRealize Automation, vérifiez que la cible ou le nouveau chemin de stockage est sélectionné dans la réservation cible de la machine avant de modifier la réservation de la machine.

Prérequis

Connectez-vous à la console de vRealize Automation en tant qu'**administrateur Fabric**.

Procédure

- 1 Sélectionnez **Infrastructure > Machines gérées**.
- 2 Localisez la machine contenant la réservation à modifier.
- 3 Cliquez sur **Modifier la réservation** dans le menu déroulant.

Vous pouvez afficher des informations sur la machine gérée, telles que son Blueprint associé et la ressource de calcul, en cliquant sur **Afficher** dans le menu déroulant.

- 4 (Facultatif) Sélectionnez un groupe d'activité dans le menu déroulant **Groupe d'activité**.

- 5 (Facultatif) Sélectionnez une réservation dans le menu déroulant **Réservation**.
- 6 (Facultatif) Sélectionnez une stratégie de stockage dans le menu déroulant **Stockage**.
- 7 Cliquez sur **OK**.

Créer un snapshot de votre machine

En fonction de la manière dont vos administrateurs ont configuré votre environnement, vous pouvez créer un snapshot de votre machine virtuelle. Un snapshot est une image d'une machine virtuelle à un moment spécifique. Il s'agit d'une copie à optimisation d'espace de l'image originale de la VM. Les snapshots constituent une manière simple de restaurer un système après un dommage, la perte de données ou des menaces de sécurité. Après avoir créé un snapshot de votre machine virtuelle, vous pouvez l'appliquer et réinitialiser votre système dans l'état dans lequel il se trouvait lorsque le snapshot a été pris.

Lorsque vous créez un snapshot de mémoire, le snapshot capture l'état des paramètres d'alimentation de la machine virtuelle et, éventuellement, la mémoire de la machine virtuelle. Lorsque vous capturez l'état de la mémoire de la machine virtuelle, l'opération de création d'un snapshot est plus longue. Il est possible que vous observiez une pause momentanée de la réponse sur le réseau.

Prérequis

- Une machine virtuelle existante mise sous tension, hors tension ou interrompue.
- Si votre machine virtuelle est configurée pour un ou plusieurs disques indépendants, mettez la machine hors tension avant de créer un snapshot. Vous ne pouvez pas créer un snapshot lorsque la machine est sous tension. Pour obtenir des informations sur la configuration de disque, reportez-vous à *Tableau des propriétés personnalisées en V*.
- Votre administrateur de locataire ou votre gestionnaire de groupe d'activité vous a autorisé à réaliser l'action de snapshot.

Procédure

- 1 Sélectionnez **Éléments > Machines**.

Vous pouvez également sélectionner **Éléments > Déploiement** et accéder à la machine dans le déploiement.

- 2 Localisez la machine pour laquelle vous souhaitez prendre un snapshot.
- 3 Dans la colonne Actions, cliquez sur la flèche vers le bas, puis sur **Afficher les détails**.
- 4 Cliquez sur **Créer un snapshot** dans le menu Action.
- 5 Entrez un nom et, éventuellement, une description.
- 6 Si vous souhaitez capturer les paramètres de mémoire et d'alimentation, sélectionnez **Inclure la mémoire**.
- 7 Cliquez sur **Soumettre**.

Se connecter à distance à une machine

Vous pouvez vous connecter à distance à une machine depuis la console vRealize Automation.

Prérequis

- Connectez-vous à la console vRealize Automation en tant que **propriétaire de la machine**, **administrateur de locataire** ou **gestionnaire de groupes d'activités**.
- Vérifiez que VMware Tools est installé.

VMware Tools doit être installé sur votre client vRealize Automation pour prendre intégralement en charge l'accès lors de la connexion avec VMware Remote Console. Si VMware Tools n'est pas installé, des problèmes peuvent se produire. Il se peut, par exemple, que le pointeur et les boutons de la souris ne fonctionnent pas après la connexion à la machine cible. Pour plus d'informations sur les version de VMware Tools prises en charge, reportez-vous à *Matrice de prise en charge de vRealize Automation*.

- Vérifiez que la machine provisionnée est sous tension.

Procédure

- 1 Sélectionnez **Éléments > Déploiement**.
- 2 Cliquez sur **Actions** dans la ligne du nom de la machine ou sélectionnez la machine et cliquez sur **Actions** sur sa page de machine.
- 3 Sélectionnez la méthode de connexion à distance.
 - Sélectionnez **Connexion de l'infrastructure à l'aide de RDP** pour vous connecter via RDP.
 - Sélectionnez **Se connecter à la console distante** pour se connecter via VMware Remote Console.
 Répondez à toutes les invites.
- 4 Cliquez sur **Se connecter** et connectez-vous à la machine en suivant les instructions.
- 5 Lorsque vous avez terminé, déconnectez-vous et fermez la fenêtre du navigateur.

Configuration des consoles distantes pour vSphere avec des certificats SSL non approuvés

Si votre déploiement de vRealize Automation utilise des certificats non approuvés, vous devez configurer votre navigateur client pour approuver le certificat avant de pouvoir utiliser les consoles distantes avec VMware Remote Console. La procédure à suivre pour cela varie selon le navigateur.

Si vRealize Automation est configuré avec un certificat SSL approuvé pour votre environnement, alors VMware Remote Console ne requiert aucune configuration supplémentaire sur les navigateurs clients. Lorsqu'un certificat du dispositif vRealize Automation est remplacé et qu'il s'agit d'un certificat approuvé, il n'est pas nécessaire de mettre à jour les informations de certificat pour le client du navigateur Web.

Si vous souhaitez remplacer le certificat, reportez-vous à la rubrique sur le remplacement d'un certificat dispositif vRealize Automation dans le guide *Administration du système* pour vRealize Automation.

Les connexions distantes utilisant VMware Remote Console pour les machines provisionnées sur vSphere sont sécurisées par les certificats du dispositif vRealize Automation via une console proxy. VMware Remote Console requiert la prise en charge de WebSockets dans le navigateur et les navigateurs doivent approuver le certificat du dispositif vRealize Automation. Le certificat peut être obtenu en accédant au dispositif virtuel de niveau racine à une adresse du formulaire <https://vra-vr.eng-mycompany.com/>.

Pour plus d'informations sur les conditions de prise en charge pour les navigateurs et vSphere, reportez-vous à la section *Matrice de prise en charge de vRealize Automation*.

Configurer Firefox pour approuver un certificat pour vRealize Automation

Les certificats du dispositif vRealize Automation non approuvés doivent être importés manuellement dans les navigateurs clients pour prendre en charge VMware Remote Console sur les clients provisionnés sur vSphere.

Pour plus d'informations sur les versions prises en charge de Firefox, reportez-vous à la *matrice de prise en charge de VMware vRealize* dans le centre d'informations vRealize Automation <https://www.vmware.com/support/pubs/vrealize-automation-pubs.html>.

Remarque Si vRealize Automation est configuré avec un certificat SSL approuvé pour votre environnement, alors VMware Remote Console ne requiert aucune configuration supplémentaire sur les navigateurs clients.

Procédure

- 1 Dans un navigateur Firefox, connectez-vous au dispositif vRealize Automation.
Un message s'affiche indiquant que le certificat n'est pas approuvé.
- 2 Choisissez l'option permettant d'afficher les informations de connexion actuelles. Cliquez sur **Afficher le certificat** pour afficher le certificat SSL actif et cliquez sur **Détails** dans le visualiseur de certificats.
- 3 Cliquez sur **Plus d'informations**, puis sur l'onglet **Sécurité** dans la page Informations sur la page.
- 4 Sélectionnez un certificat dans le volet Hiérarchie de certificats.

Option	Action
Certificats émis par une autorité de certification	Sélectionnez le certificat vRealize Automation de niveau supérieur.
Certificats autosignés	Sélectionnez le certificat vRealize Automation.

- 5 Cliquez sur **Exporter**.
- 6 Configurez les informations de certificat dans la zone de texte Enregistrer le certificat dans un fichier.
 - a Entrez un nom de certificat dans la zone de texte **Enregistrer sous**. Le nom de certificat doit se terminer par .crt, .cert ou .cer.
 - b Sélectionnez un emplacement où enregistrer le fichier.
 - c Sélectionnez le format **Certificat X.509 (PEM)**.

7 Cliquez sur **Enregistrer**.

8 Dans la zone de texte Gestion des certificats, cliquez sur l'onglet **Autorités**.

Option	Action
Windows	Dans le menu Firefox, sélectionnez Préférence > Avancé > Certificats .
iOS	Dans le menu Firefox, sélectionnez Préférence > Avancé > Certificats et cliquez sur Afficher les certificats .

9 Cliquez sur l'onglet **Autorités**, puis sur **Importer**.

10 Sélectionnez le fichier de certificat enregistré précédemment et cliquez sur **Ouvrir** dans la zone de texte.

11 Modifier les paramètres de confiance.

Option	Action
Certificats autosignés	Sélectionnez Ce certificat peut identifier des sites Web .
Certificats émis par une autorité de certification	Sélectionnez Approuver cette autorité de certification pour identifier les sites Web .

12 Cliquez sur **OK**, puis redémarrez le navigateur.

Vous pouvez vous connecter à la console distante sans erreurs de certificat.

Configurer Internet Explorer pour approuver un certificat pour un dispositif vRealize Automation

Les certificats dispositif vRealize Automation non approuvés doivent être importés manuellement dans les navigateurs clients pour prendre en charge VMware Remote Console sur les clients provisionnés sur vSphere.

Remarque Si vRealize Automation est configuré avec un certificat SSL approuvé pour votre environnement, alors VMware Remote Console ne requiert aucune configuration supplémentaire sur les navigateurs clients.

Les étapes de cette procédure s'appliquent aux certificats autosignés et aux certificats émis par une autorité de certification.

Pour plus d'informations sur les versions d'Internet Explorer prises en charge, reportez-vous à *VMware vRealize Support Matrix* sur le site Web VMware.

Procédure

- 1 Dans un navigateur Internet Explorer, connectez-vous au dispositif vRealize Automation.
- 2 Cliquez sur **Afficher le certificat** dans le message d'erreur du certificat qui s'affiche dans la barre d'adresse du navigateur.
- 3 Cliquez sur l'onglet **Général** de la fenêtre Informations de certificat.

- 4 Vérifiez que les informations concernant le certificat sont correctes et cliquez sur **Installer le certificat**.
- 5 Sélectionnez **Placer tous les certificats dans le magasin suivant** dans la boîte de dialogue du magasin de certificats.
- 6 Cliquez sur **Parcourir** pour localiser le magasin de certificats.
- 7 Sélectionnez **Autorité de certification racine approuvée** et cliquez sur **OK**.
- 8 Cliquez sur **Suivant** dans la boîte de dialogue du magasin de certificats.
- 9 Cliquez sur **Oui** dans la boîte de dialogue d'avertissement de sécurité pour installer le certificat.
- 10 Redémarrez le navigateur.

Vous pouvez vous connecter à la console distante sans erreurs de certificat.

Configurer Chrome pour approuver un certificat pour un dispositif vRealize Automation

Les certificats dispositif vRealize Automation non approuvés doivent être importés manuellement dans les navigateurs clients pour prendre en charge VMware Remote Console sur les clients provisionnés sur vSphere.

Pour plus d'informations sur les versions de Chrome prises en charge, reportez-vous à *VMware vRealize Support Matrix* sur le site Web VMware.

Remarque Si vRealize Automation est configuré avec un certificat SSL approuvé pour votre environnement, alors VMware Remote Console ne requiert aucune configuration supplémentaire sur les navigateurs clients.

Sur Windows, Chrome et Internet Explorer utilisent le même magasin de certificats. Cela signifie que les certificats approuvés par Internet Explorer le sont également par Chrome. Pour établir des certificats approuvés pour Chrome, importez-les via Internet Explorer. Pour plus d'informations sur cette procédure, reportez-vous au document [Configurer Internet Explorer pour approuver un certificat pour un dispositif vRealize Automation](#).

Lorsque vous terminez la procédure, redémarrez Chrome.

Pour approuver un certificat de manière définitive sur un système d'exploitation Macintosh, téléchargez le fichier de certificat et installez-le comme élément approuvé dans votre outil de gestion des certificats.

Procédure

- 1 Dans un navigateur Chrome, connectez-vous au dispositif vRealize Automation.
- 2 Cliquez sur l'icône dans la barre d'adresse.
- 3 Cliquez sur le lien d'informations de certificat.
- 4 Enregistrez le certificat en faisant glisser l'icône de certificat vers le bureau.
- 5 Démarrez l'application Keychain Access.
- 6 Sélectionnez **Fichier > Importer des éléments**.

- 7 Sur l'écran de Keychain Access, sélectionnez le fichier de certificat enregistré précédemment.
Réglez la valeur de **Clé de destination** sur **Système**.
- 8 Cliquez sur **Ouvrir** pour importer le certificat.
- 9 Redémarrez le navigateur.

Forcer la destruction d'un déploiement après l'échec d'une demande de destruction

Vous pouvez forcer la destruction d'un déploiement dont l'état est incohérent suite à une demande de destruction ayant échoué.

Lorsque vRealize Automation ne parvient pas à détruire une ressource de déploiement lors d'une opération de déploiement de destruction, l'opération de destruction s'arrête immédiatement sans détruire les ressources de déploiement restantes. Cet échec laisse le déploiement dans un état incohérent et utilise des ressources sans aucun moyen évident de détruire le déploiement. Les administrateurs de groupes d'activités peuvent forcer la destruction des déploiements qui se retrouvent dans cet état incohérent.

Prérequis

Vérifiez que vous êtes connecté à vRealize Automation en tant qu'**administrateur du groupe d'activité**.

Procédure

- 1 Dans l'onglet **Éléments**, cliquez sur **Déploiements** et sélectionnez le déploiement à détruire.
- 2 Cliquez sur **Actions**, puis cliquez sur **Détruire**.
- 3 Entrez la description et la raison de la demande.
- 4 Sélectionnez **Forcer la destruction** et cliquez sur **Envoyer**.

vRealize Automation tente de détruire entièrement le déploiement, y compris toutes les ressources dans le déploiement. Si vRealize Automation ne parvient pas à détruire une ressource de déploiement, il ignore cette ressource et continue à détruire les ressources restantes dans le déploiement.

Suivant

Cliquez sur l'onglet **Demandes** et vérifiez que toutes les ressources dans le déploiement ont été correctement détruites. Toutes les ressources qui n'ont pas été détruites lors d'une opération de destruction forcée doivent être détruites manuellement. Assurez-vous également que tous les objets de machine virtuelle provisionnée sont détruits, car vRealize Automation peut tenter de réutiliser leurs noms d'hôte, adresses IP et autres détails de configuration pendant les opérations de provisionnement suivantes.

Dépannage des actions manquantes dans le menu Actions sur les ressources

En tant que propriétaire de machine ou de ressource, vous ne voyez pas toutes les actions autorisées pour un élément provisionné.

Problème

Dans un environnement où vous savez qu'une action est autorisée pour votre utilisateur ou votre groupe d'activité, vous vous attendez à voir toutes les actions lorsque vous sélectionnez un élément dans votre liste **Éléments**.

Cause

La disponibilité des actions dépend du type de ressource provisionnée, de l'état opérationnel de la ressource et de la manière dont elle a été configurée et mise à disposition. La liste suivante indique un certain nombre de raisons pour lesquelles vous ne voyez pas toutes les actions configurées.

- L'action ne s'applique pas à l'état actuel de la ressource provisionnée. Par exemple, Mettre hors tension est uniquement disponible lorsque la machine est sous tension.
- L'action ne s'applique pas au type d'élément sélectionné. Si l'élément ne prend pas en charge l'action, celle-ci n'est pas affichée dans la liste. Par exemple, l'action Créer un snapshot n'est pas disponible pour une machine physique et l'action Se connecter via RDP n'est pas disponible si l'élément sélectionné est une machine Linux.
- L'action s'applique au type de ressource provisionnée, mais elle est désactivée dans le Blueprint de l'infrastructure. Si l'action est désactivée, elle n'est jamais affichée comme action disponible pour aucun élément provisionné au moyen du Blueprint.
- L'action n'est pas comprise dans le droit d'accès utilisé pour provisionner l'élément sur lequel vous devez exécuter l'action. Seules les actions autorisées, que ce soit dans le cadre d'un Blueprint IaaS ou d'une action de ressource XaaS, peuvent s'afficher dans le menu Actions.
- L'action est créée comme une action de ressource XaaS mais n'est pas comprise dans le droit d'accès utilisé pour provisionner l'élément sur lequel vous devez exécuter l'action. Seules les actions autorisées s'affichent dans le menu Actions.
- L'action peut être limitée selon le critère cible configuré pour les actions de ressources XaaS ou les mappages de ressources pour les machines IaaS provisionnées.

Solution

- Vérifiez que l'action s'applique à l'élément provisionné ou à l'état de l'élément provisionné.
- Vérifiez que l'action est configurée et comprise dans le droit d'accès utilisé pour provisionner l'élément.

Dépannage d'un échec de déploiement qui inclut un workflow vRealize Orchestrator

Si un déploiement de Blueprint ayant échoué comprend un workflow vRealize Orchestrator, vous pouvez utiliser l'ID de jeton pour résoudre les problèmes avec le workflow. L'ID de jeton vous permet de localiser les journaux dans vRealize Orchestrator.

Solution

- 1 Recherchez l'ID de jeton du workflow ayant échoué.
 - a Dans vRealize Automation, cliquez sur l'onglet **Demande**.
 - b Cliquez sur le nombre dans la colonne Demande.
La demande peut être un déploiement ou une action.
 - c Cliquez sur l'onglet **Général**.
Si le Blueprint est basé sur un workflow vRealize Orchestrator, le titre de la page est Détails de l'exécution du workflow vRealize Orchestrator.
 - d Recherchez l'ID de jeton et copiez-le dans le presse-papiers ou un fichier texte.
Par exemple, ff8080815a685352015a6c8d450801ee.
- 2 Localiser les journaux de workflow dans vRealize Orchestrator en utilisant le centre de contrôle
 - a Entrez l'URL de base de vRealize Automation dans la zone de recherche du navigateur.
La page du dispositif vRealize Automation VMware s'affiche.
 - b Cliquez sur **Centre de contrôle vRealize Orchestrator**.
 - c Connectez-vous en tant qu'utilisateur disposant de privilèges racine.
 - d Cliquez sur **Inspecter les Workflows**.
 - e Cliquez sur **Workflows terminés**.
 - f Collez le jeton du workflow dans la zone de texte ID de jeton.
La liste s'affiche sur le workflow qui correspond à l'ID de jeton.
 - g Cliquez sur la ligne et inspecter les journaux pour connaître la cause de l'échec.

Spécifiez les paramètres de reconfiguration de machine et les éléments à prendre en compte pour la reconfiguration

Les plates-formes vSphere, vCloud Air et vCloud Director prennent en charge la reconfiguration de machines existantes dans un déploiement pour modifier des spécifications telles que le CPU, la mémoire et le stockage.

Les demandes de reconfiguration sont soumises à approbation en fonction des droits d'accès, des stratégies et des actions activées pour le composant de machine dans le Blueprint.

La reconfiguration d'une machine virtuelle qui est attribuée à un réseau à la demande n'est pas prise en charge. Vous ne pouvez pas reconfigurer une carte réseau qui est associée à un réseau à la demande. Si vous tentez de reconfigurer un réseau NAT à la demande ou un réseau routé, le message d'erreur 'Original network [<network>] is not selected in the machine's reservation. s'affiche, les réseaux sur la machine restent intacts et les adresses IP sur la machine restent inchangées.

Si vous avez accès aux actions Annuler la reconfiguration (Machine) et Exécuter la reconfiguration (Machine), vous pouvez annuler ou réessayer une reconfiguration ayant échoué.

L'expansion d'un disque sur une machine virtuelle qui a été provisionnée à partir d'un Blueprint de clone lié n'est pas prise en charge.

Vous ne pouvez pas reconfigurer les machines à l'aide des profils de composants Size ou Image, mais la plage de CPU, de la mémoire et du stockage qui est calculée en fonction du profil reste disponible pour des actions de reconfiguration. Par exemple, si vous avez utilisé un petit (1 CPU, 1 024 Mo de mémoire et 10 Go de stockage), moyen (3 CPU, 2 048 Mo de mémoire et 12 Go de stockage) et grand (5 CPU, 3 072 Mo de mémoire et 15 Go de stockage) ensemble de valeurs Size, les plages disponibles pendant la reconfiguration de la machine sont 1 à 5 CPU, 1 024 à 3 072 Mo de mémoire et 1 à 15 Go de stockage.

vRealize Automation prend un snapshot de Blueprint au moment du déploiement. Si vous rencontrez des problèmes de reconfiguration lors de la mise à jour des propriétés de la machine telles que le CPU et la RAM de la machine dans un déploiement, consultez l'article de la base de connaissances [2150829 vRA 7.x Blueprint Snapshotting](#).

Prérequis

- Connectez-vous à la console vRealize Automation en tant que **propriétaire de la machine, utilisateur de support technique, utilisateur de groupe d'activité avec un rôle d'accès partagé** ou de **gestionnaire de groupe d'activité**.
- La machine que vous souhaitez reconfigurer doit être sous tension ou hors tension et ne pas être dans un état de reconfiguration actif.
- Le type de machine doit être vSphere, vCloud Air ou vCloud Director bien que les paramètres NSX s'appliquent uniquement à vSphere.
- Vérifiez que vous êtes autorisé à reconfigurer une machine.

Procédure

- 1 Sélectionnez **Éléments > Machines**.

Vous pouvez également sélectionner **Éléments > Déploiement** et accéder à la machine dans le déploiement.

- 2 Sélectionnez la machine à reconfigurer



- 3 Sélectionnez **Reconfigurer** dans le menu **Actions**.
- 4 Sélectionnez l'onglet approprié pour les paramètres que vous souhaitez reconfigurer.

Tableau 3-76. Demander des modifications de reconfiguration

Onglet	Rubrique
Général	Reconfigurer les CPU et la mémoire
Stockage	Modifier les paramètres de stockage

Tableau 3-76. Demander des modifications de reconfiguration (suite)

Onglet	Rubrique
Réseau	Modifier les paramètres réseau Pour modifier les règles NAT, reportez-vous à la section Modifier les règles NAT dans un déploiement .
Sécurité	Pour reconfigurer les paramètres de sécurité, reportez-vous à la section Ajouter ou supprimer des éléments de sécurité dans un déploiement .
Propriétés	Modifier les paramètres des propriétés personnalisées et de groupe de propriétés

Suivant

[Exécuter la reconfiguration de machine demandée.](#)

Reconfigurer les CPU et la mémoire

Vous pouvez modifier le nombre de CPU ou la quantité de mémoire et de stockage utilisée par la machine provisionnée, dans les limites définies par le Blueprint de provisionnement.

Pour les déploiements Amazon provisionnés, vous pouvez reconfigurer tous les volumes de stockage dans le déploiement à l'exception du volume racine.

L'expansion d'un disque sur une machine virtuelle qui a été provisionnée à partir d'un Blueprint de clone lié n'est pas prise en charge.

Prérequis

[Spécifiez les paramètres de reconfiguration de machine et les éléments à prendre en compte pour la reconfiguration.](#)

Procédure

- 1 Cliquez sur l'onglet **Général**.
- 2 Entrez le nombre de CPU dans la zone de texte **Nbre de CPU**.
- 3 Entrez la quantité de mémoire dans la zone de texte **Mémoire (Mo)**.
- 4 Entrez la quantité de stockage dans la zone de texte **Stockage (Mo)**.

Suivant

Spécifiez les paramètres de reconfiguration de machine supplémentaires. Si vous avez terminé de modifier les paramètres de machine, démarrez la demande de reconfiguration de machine. Reportez-vous à [Exécuter la reconfiguration de machine demandée](#).

Modifier les paramètres de stockage

Vous pouvez ajouter, supprimer ou modifier la taille d'un volume de stockage sur une machine virtuelle provisionnée.

Vous ne pouvez pas reconfigurer le stockage pour le type de disque IDE.

Le stockage et la mémoire alloués à une machine provisionnée via une réservation sont libérés lorsque la machine est supprimée dans vRealize Automation par l'action Détruire. Le stockage et la mémoire ne sont pas libérés si la machine est supprimée dans vCenter Server.

Par exemple, vous ne pouvez pas supprimer une réservation associée aux machines d'un déploiement existant. Si vous déplacez ou supprimez des machines déployées manuellement dans vCenter Server, vRealize Automation continue de reconnaître les machines déployées comme étant en temps réel et vous empêche de supprimer les réservations associées.

Prérequis

Spécifiez les paramètres de reconfiguration de machine et les éléments à prendre en compte pour la reconfiguration.

Pour les déploiements Amazon provisionnées, vous pouvez reconfigurer tous les volumes de stockage dans le déploiement à l'exception du volume racine.

Procédure

- 1 Cliquez sur l'onglet **Stockage**.

La plage de stockage autorisée s'affiche sous le tableau Volumes de stockage.

- 2 Ajoutez ou modifiez les paramètres de volume de stockage disponible.

- a Cliquez sur **Nouveau volume**.
- b Tapez la capacité dans la zone de texte **Capacité (Go)**.
- c Sélectionnez une stratégie de réservation de stockage dans le menu déroulant **Stratégie de réservation de stockage**.
- d Cliquez sur l'icône **Enregistrer** (✓).

- 3 Supprimez un volume.

- a Recherchez le volume.
- b Cliquez sur l'icône **Supprimer** (🗑).

Une icône non sélectionnable indique un volume ne pouvant pas être supprimé comme un volume de clone lié.

- 4 Augmentez la taille d'un volume.

Vous ne pouvez pas réduire la taille des volumes existants. La taille du volume est limitée par la quantité totale de stockage spécifiée dans le Blueprint, moins la quantité allouée aux autres volumes.

- a Recherchez le volume.
- b Cliquez sur l'icône **Modifier** (✎).

- c Tapez la nouvelle taille dans la zone de texte **Capacité (Go)**.
- d Cliquez sur l'icône **Enregistrer** (✓).

Suivant

Spécifiez les paramètres de reconfiguration de machine supplémentaires. Si vous avez terminé de modifier les paramètres de machine, démarrez la demande de reconfiguration de machine. Reportez-vous à [Exécuter la reconfiguration de machine demandée](#).

Modifier les paramètres réseau

Vous pouvez ajouter, supprimer ou modifier un adaptateur réseau.

Vous pouvez modifier les paramètres réseau suivants pendant le processus de reconfiguration de la machine :

- Ajoutez ou supprimez des cartes réseau.
- Allouez ou libérez des adresses IP pour les cartes réseau existantes.
- Attribuez les nouvelles adresses IP aux cartes réseau, sous réserve que le réseau n'est pas un NAT à la demande ou un réseau routé à la demande.

Vous ne pouvez pas reconfigurer un réseau NAT routé à la demande ou un réseau NAT à la demande.

La reconfiguration du réseau nécessite que les réseaux source et cible soient sélectionnés dans la réservation.

Lorsque vous ajoutez des cartes réseau, des adresses IP sont allouées. Lorsque vous supprimez des cartes réseau, des adresses IP sont libérées.

Lorsque vous modifiez des paramètres réseau en fonction des informations de la réservation et du profil réseau, l'adresse IP du réseau est attribuée à vRealize Automation mais la machine déployée n'est pas mise à jour sur le point de terminaison avec les informations de la nouvelle adresse IP. Vous devez attribuer manuellement l'adresse IP à la machine lorsque le processus de reconfiguration est terminé.

La reconfiguration d'une machine virtuelle qui est attribuée à un réseau à la demande n'est pas prise en charge. Vous ne pouvez pas reconfigurer une carte réseau qui est associée à un réseau à la demande. Si vous tentez de reconfigurer un réseau NAT à la demande ou un réseau routé, le message d'erreur 'Original network [<network>] is not selected in the machine's reservation.' s'affiche, les réseaux sur la machine restent intacts et les adresses IP sur la machine restent inchangées.

La modification des paramètres réseau NSX n'est pas prise en charge pour les déploiements mis à niveau ou migrés depuis vRealize Automation 6.2.x vers cette version de vRealize Automation.

Prérequis

[Spécifiez les paramètres de reconfiguration de machine et les éléments à prendre en compte pour la reconfiguration.](#)

Procédure

- 1 Cliquez sur l'onglet **Réseau**.
- 2 (Facultatif) Ajoutez un adaptateur réseau.
 - a Cliquez sur **Nouvel adaptateur réseau**.
 - b Choisissez un réseau dans le menu déroulant **Chemin réseau**.
Tous les réseaux sélectionnés dans la réservation de la machine sont disponibles.
 - c Tapez une adresse IP statique pour le réseau dans la zone de texte **Adresse**.
L'adresse IP doit être non allouée dans le profil réseau attribué dans la réservation.
 - d Cliquez sur l'icône **Enregistrer** (✓).
- 3 (Facultatif) Supprimez un adaptateur réseau.
 - a Recherchez l'adaptateur réseau.
 - b Cliquez sur l'icône **Supprimer** (🗑️).

Vous ne pouvez pas supprimer l'adaptateur réseau 0.
- 4 (Facultatif) Modifiez un adaptateur réseau.
 - a Recherchez l'adaptateur réseau.
 - b Cliquez sur l'icône **Modifier** (✎).
 - c Choisissez un réseau dans le menu déroulant **Chemin réseau**.
 - d Cliquez sur l'icône **Enregistrer** (✓).

Suivant

Spécifiez les paramètres de reconfiguration de machine supplémentaires. Si vous avez terminé de modifier les paramètres de machine, démarrez la demande de reconfiguration de machine. Reportez-vous à [Exécuter la reconfiguration de machine demandée](#).

Modifier les paramètres des propriétés personnalisées et de groupe de propriétés

Vous pouvez modifier, ajouter ou supprimer des propriétés personnalisées dans la machine déployée.

Vous ne pouvez pas utiliser les propriétés personnalisées pour entrer des valeurs pour le numéro de volume de disque, l'étiquette de capacité ou la stratégie de réservation de stockage. Vous devez entrer ces valeurs en ajoutant ou en modifiant un volume dans le tableau Volumes de stockage. Reportez-vous à [Modifier les paramètres de stockage](#).

Prérequis

[Spécifiez les paramètres de reconfiguration de machine et les éléments à prendre en compte pour la reconfiguration.](#)

Procédure

- 1 Cliquez sur l'onglet **Propriétés**.
- 2 Pour ajouter une propriété, cliquez sur **Nouvelle propriété**.
- 3 Entrez le nom de la propriété dans la zone de texte **Nom**.
- 4 Entrez la valeur de la propriété dans la zone de texte **Valeur**.
- 5 Cochez la case **Chiffré** pour chiffrer la valeur.
- 6 Cochez la case **Inviter l'utilisateur** pour demander à l'utilisateur la valeur lorsqu'il demande la machine.
- 7 Ajoutez une autre propriété, modifiez une propriété existante ou supprimez une propriété.

Suivant

Spécifiez les paramètres de reconfiguration de machine supplémentaires. Si vous avez terminé de modifier les paramètres de machine, démarrez la demande de reconfiguration de machine. Reportez-vous à [Exécuter la reconfiguration de machine demandée](#).

Exécuter la reconfiguration de machine demandée

Vous pouvez démarrer la reconfiguration de machine demandée immédiatement ou la planifier pour démarrer à une date et une heure spécifiques. Vous pouvez également spécifier l'option d'alimentation de la machine avant de la reconfigurer.

Prérequis

[Spécifiez les paramètres de reconfiguration de machine et les éléments à prendre en compte pour la reconfiguration.](#)

Procédure

- 1 Si l'onglet **Exécution** est visible, vous pouvez le sélectionner pour spécifier des paramètres de reconfiguration supplémentaires. S'il n'est pas visible, cliquez sur **Envoyer** pour démarrer la reconfiguration de machine.
- 2 Si l'onglet **Exécution** est visible, cliquez sur **Exécution** pour planifier l'action de reconfiguration.
- 3 (Facultatif) Sélectionnez une option dans le menu déroulant **Exécuter la demande**.

Option	Description
Urgent	Démarrer la reconfiguration dès que possible après l'approbation.
Planifié	Démarrer la reconfiguration à la date et à l'heure spécifiées. Tapez ou sélectionnez la date et l'heure dans les zones de texte qui s'affichent.

L'heure planifiée est l'heure locale à laquelle se trouve le serveur Web vRealize Automation. Si **Exécuter la demande** n'est pas disponible, la reconfiguration démarrera immédiatement.

4 (Facultatif) Sélectionnez une action d'alimentation dans le menu déroulant **Action d'alimentation**.

Option	Description
Redémarrer au besoin	(Par défaut) Au besoin, redémarrez la machine avant de la reconfigurer.
Redémarrage	Redémarrez la machine avant de la reconfigurer, que le redémarrage soit requis ou non.
Ne pas redémarrer	Ne redémarrez pas la machine avant de la reconfigurer, même si le redémarrage est requis.

Les conditions suivantes nécessitent que la machine soit redémarrée avant la reconfiguration :

- Changement de CPU au cours duquel l'ajout à chaud n'est pas pris en charge ou est désactivé
- Changement de mémoire au cours duquel la mémoire à chaud n'est pas prise en charge ou est désactivée
- Changement de stockage au cours duquel le stockage à chaud est désactivé

Si la machine est à l'arrêt, elle n'est pas redémarrée.

Remarque Vous pouvez désactiver l'option d'ajout à chaud de vSphere à l'aide la propriété personnalisée `VirtualMachine.Reconfigure.DisableHotCpu`.

5 Cliquez sur **OK**.

Suivant

Vous pouvez surveiller la progression de la reconfiguration en observant les états du workflow s'afficher dans l'interface utilisateur. Reportez-vous à [États de workflow des opérations de reconfiguration](#).

États de workflow des opérations de reconfiguration

Au démarrage de la reconfiguration et au fur et à mesure qu'elle progresse dans le workflow, vous pouvez surveiller sa progression dans la page Modifier.

Tableau 3-77. États de workflow des opérations de reconfiguration

État	Description
Reconfiguration en attente	L'opération d'état a été créée.
Planifié	Un workflow planifié a été créé pour le DEM.
Reconfiguration en cours	Le workflow spécifique à l'interface est en cours d'exécution.
Échec de la reconfiguration, en attente de renouvellement	La reconfiguration a échoué et attend que le propriétaire demande une nouvelle tentative. Si le propriétaire de la machine est autorisé à ordonner les actions Exécuter la reconfiguration ou Annuler la reconfiguration, il peut réessayer ou annuler une reconfiguration.
ReconfigureFailed	La reconfiguration a échoué, dans l'attente que le workflow RVG effectue l'action suivante.
ReconfigureSuccessful	La reconfiguration a réussi, dans l'attente que le workflow RVG effectue l'action suivante.

Tableau 3-77. États de workflow des opérations de reconfiguration (suite)

État	Description
Annulé	L'utilisateur a annulé la reconfiguration. Les propriétaires de machines autorisés à effectuer l'action Annuler la reconfiguration peuvent annuler la reconfiguration.
Terminé	Le workflow d'achèvement définit cet état après avoir terminé le nettoyage, de sorte que le workflow RVG puisse procéder au nettoyage des opérations et des approbations d'états. Un état Terminé indique que la demande de vRealize Automation est terminée, mais il n'indique pas si la reconfiguration de la machine s'est terminée avec succès.

Reconfigurer un équilibrage de charge dans un déploiement

Vous pouvez ajouter, modifier ou supprimer un serveur virtuel dans un équilibrage de charge NSX déployé.

Les éléments à prendre en compte suivants s'appliquent aux déploiements ayant pour origine vRealize Automation 7.2 ou version antérieure :

- La reconfiguration d'équilibrage de charge est limitée aux déploiements qui contiennent un équilibrage de charge unique.
- La page Détails de l'élément d'un équilibrage de charge dans un déploiement affiche les serveurs virtuels utilisés par tous les équilibrateurs de charge dans le déploiement. Pour plus d'informations, reportez-vous à [l'article 2150276 de la base de connaissances](#).

Pour les équilibres de charge mis à niveau et les équilibres de charge déployés dans la version actuelle de vRealize Automation, ne modifiez pas et n'ajoutez pas de serveur virtuel dans la même demande. Pour plus d'informations, reportez-vous à [l'article 2150240 de la base de connaissances](#).

Si vous envoyez une demande visant à reconfigurer un équilibrage de charge pendant l'exécution d'une autre action sur le déploiement, par exemple quand une opération de montée en charge sur le déploiement est en cours, la reconfiguration échoue avec un message de soutien. Dans ce cas, vous pouvez attendre la fin de l'action, puis soumettre la demande de reconfiguration.

L'opération Reconfigurer l'équilibrage de charge n'est pas prise en charge pour les déploiements mis à niveau ou migrés depuis vRealize Automation 6.2.x vers cette version vRealize Automation.

Vous ne devez pas gérer les objets NSX administrés par vRealize Automation en dehors de vRealize Automation. Par exemple, si vous modifiez le port membre d'un équilibrage de charge NSX déployé dans NSX, plutôt que dans vRealize Automation, la collecte de données NSX rompt l'association entre la machine déployée et son pool de membres de l'équilibrage de charge associé ailleurs. Les opérations de réduction de charge et de montée en charge génèrent également des résultats inattendus si un port membre de l'équilibrage de charge déployé est modifié à l'extérieur de vRealize Automation.

Reportez-vous aux vRealize Automation [notes de mise à jour](#) pour tout problème connu.

Pour plus d'informations sur les paramètres qui sont disponibles lorsque vous ajoutez ou modifiez un serveur virtuel, reportez-vous à la section [Ajouter un composant d'équilibrage de charge à la demande](#).

Lorsque vous reconfigurez un équilibrage de charge dans vRealize Automation, certains des paramètres qui ont été configurés dans NSX et qui ne sont pas disponibles en tant que paramètres dans vRealize Automation sont restaurés à leur valeur par défaut. Après avoir exécuté l'action de reconfiguration d'équilibrage de charge dans vRealize Automation, vérifiez et mettez éventuellement à jour les paramètres suivants dans NSX :

- En-tête Insert-X-Forwarded for HTTP
- URL de redirection HTTP
- Extension de moniteur de services

Prérequis

- Connectez-vous à la console vRealize Automation en tant que **propriétaire de la machine, utilisateur de support technique, utilisateur de groupe d'activité avec un rôle d'accès partagé** ou de **gestionnaire de groupe d'activité**.
- Vérifiez que vous êtes autorisé à reconfigurer des équilibres de charge dans un déploiement. Le droit d'accès de catalogue requis est Reconfigurer (Équilibrage de charge).

Procédure

- 1 Sélectionnez **Éléments > Déploiement**.
- 2 Localisez le déploiement et affichez ses composants enfants.



- 3 Sélectionnez l'équilibrage de charge NSX à modifier.

Item Details



- 4 Sélectionnez **Reconfigurer** dans le menu **Actions**.
- 5 Ajoutez, modifiez ou supprimez des serveurs virtuels.

Virtual servers: + N... E... X Del...

Protocol	Port	Description	Member Protocol	Member Port	Health Check Protocol	Health Check Port
HTTP	80		HTTP	80	HTTP	80
HTTP	81		HTTP	81	HTTP	81

- 6 Lorsque vous avez terminé d'ajouter, de modifier ou de supprimer des serveurs virtuels, cliquez sur **Envoyer** pour envoyer la demande de reconfiguration.

Modifier les règles NAT dans un déploiement

Vous pouvez ajouter, modifier et supprimer les règles NAT existantes de NSX dans un réseau NAT déployé un à plusieurs. Vous pouvez également modifier l'ordre dans lequel les règles NAT sont traitées.

Pour plus d'informations sur les règles NAT, reportez-vous aux sections [Création et utilisation de règles NAT](#) et [Ajouter un composant réseau NAT à la demande ou routé à la demande](#).

L'opération de modification des règles NAT n'est pas prise en charge pour les déploiements qui ont été mis à niveau ou migrés depuis vRealize Automation 6.2.x vers cette version de vRealize Automation.

Vous ne pouvez pas ajouter une règle NAT à un déploiement qui est mappé à un point de terminaison IPAM tiers tel qu'Infoblox.

Reportez-vous aux notes de mise à jour de vRealize Automation

<https://www.vmware.com/support/pubs/vrealize-automation-pubs.html> pour tout problème connu.

Prérequis

- Connectez-vous à la console vRealize Automation en tant que **propriétaire de la machine**, **utilisateur de support technique**, **utilisateur de groupe d'activité avec un rôle d'accès partagé** ou de **gestionnaire de groupe d'activité**.
- Vérifiez que vous êtes autorisé à modifier les règles NAT dans un réseau.
- Le réseau NAT doit être configuré comme un réseau NAT un à plusieurs. Cette action n'est pas disponible pour les réseaux NAT un à un. Reportez-vous à

Procédure

- 1 Sélectionnez **Éléments > Déploiement**.
- 2 Localisez le déploiement et affichez ses composants enfants.



- 3 Sélectionnez le composant réseau NAT à modifier.



- 4 Dans le menu **Actions**, cliquez sur **Modifier des règles NAT**.



- 5 Ajoutez de nouvelles règles de réacheminement de port NAT, changez l'ordre des règles, modifiez les règles existantes ou supprimez des règles.
- 6 Une fois les modifications appliquées, cliquez sur **Enregistrer** ou sur **Envoyer** pour envoyer la demande de reconfiguration.

Ajouter ou supprimer des éléments de sécurité dans un déploiement

Vous pouvez ajouter ou supprimer des balises de sécurité et des groupes de sécurité NSX existants dans un déploiement de machine. Vous ne pouvez pas ajouter de groupes de sécurité à la demande, mais vous pouvez en supprimer.

L'action Modifier la sécurité est basée sur un composant de machine ou un cluster. Par exemple, si la sécurité est associée à un cluster nommé AppTier2 comprenant deux machines, vous effectuez l'opération de modification de la sécurité sur le cluster AppTier2 et non sur les machines individuelles contenues dans le cluster.

L'opération Modifier la sécurité n'est pas prise en charge pour les déploiements mis à niveau ou migrés de vRealize Automation 6.2.x vers cette version vRealize Automation.

Prérequis

- Connectez-vous à la console vRealize Automation en tant que **propriétaire de la machine, utilisateur de support technique, utilisateur de groupe d'activité avec un rôle d'accès partagé** ou de **gestionnaire de groupe d'activité**.
- Vérifiez que vous êtes autorisé à modifier la sécurité dans un déploiement. Le droit d'accès aux catalogues est Modifier la sécurité (déploiement).

Procédure

- 1 Sélectionnez **Éléments > Déploiement**.
- 2 Localisez le déploiement et affichez ses composants enfants.



- 3 Cliquez sur **Modifier la sécurité** dans le menu **Actions**.



- 4 Sélectionnez le composant de machine déployée ou le cluster dans lequel ajouter ou supprimer des éléments de sécurité.



- 5 Ajoutez ou supprimez des groupes de sécurité et des balises de sécurité pour chaque composant de machine ou cluster inclus dans le déploiement, selon vos besoins.
- 6 Supprimez des groupes de sécurité à la demande pour chaque composant de machine ou cluster inclus dans le déploiement, selon vos besoins.
- 7 (Facultatif) Cliquez sur l'onglet **Motif** et saisissez le motif de la demande.
- 8 Une fois vos modifications effectuées, cliquez sur **Enregistrer** ou cliquez sur **Envoyer** pour envoyer la demande de modification.

Afficher toutes les règles NAT pour un dispositif NSX Edge existant

Vous pouvez afficher des informations sur la règle NAT pour les dispositifs NSX Edge qui sont utilisés dans des déploiements actifs.

Les règles NAT sont affichées dans la vue Edge sous forme d'agrégat de toutes les règles NAT qui sont utilisées dans le déploiement. Dans la vue Edge, les règles ne s'affichent pas nécessairement dans l'ordre dans lequel elles sont traitées.

Pour afficher, et éventuellement modifier, l'ordre dans lequel les règles NAT sont traitées dans un réseau NAT de type un-à-plusieurs, reportez-vous à [Modifier les règles NAT dans un déploiement](#).

Prérequis

- Connectez-vous à la console vRealize Automation en tant que **propriétaire de la machine**, **utilisateur de support technique**, **utilisateur de groupe d'activité avec un rôle d'accès partagé** ou de **gestionnaire de groupe d'activité**.

Procédure

- 1 Sélectionnez **Éléments > Déploiement**.
- 2 Localisez le déploiement et affichez ses composants enfants.



- 3 Sélectionnez le dispositif NSX Edge que vous souhaitez afficher.



- 4 Lorsque vous avez terminé, cliquez sur **Fermer**.