

Installation de vRealize Automation

21 juillet 2021

vRealize Automation 7.5

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

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

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

VMware France SAS.
Tour Franklin
100-101 Terrasse Boieldieu
92042 Paris La Défense 8 Cedex
France
www.vmware.com/fr

Copyright © 2014-2021 VMware, Inc. Tous droits réservés. [Informations relatives aux copyrights et marques commerciales.](#)

Table des matières

Installation de vRealize Automation 7

Informations mises à jour 8

1 Présentation de l'installation 10

À propos de l'installation 10

Nouveautés dans cette installation 11

Composants d'installation 11

Le dispositif vRealize Automation 11

IaaS (Infrastructure en tant que service) 12

Type de déploiement 15

Déploiements minimaux 15

Déploiements distribués 16

Choisir votre méthode d'installation 19

2 Préparation à l'installation 20

Préparation générale 20

Comptes et mots de passe 21

Noms d'hôtes et adresses IP 23

Latence et bande passante 24

Dispositif vRealize Automation 25

Ports du dispositif vRealize Automation 25

Serveurs Windows IaaS 28

Ports de serveur Windows IaaS 29

Serveur Web IaaS 30

Hôte Manager Service IaaS 32

Hôte du serveur SQL IaaS 32

Hôte DEM (Distributed Execution Manager) IaaS 33

DEM Workers avec Amazon Web Services 33

DEM Workers avec Openstack ou PowerVC 33

DEM Workers avec virtualisation Red Hat 34

DEM Workers avec SCVMM 35

Certificats 36

Exigences en matière de certificats vRealize Automation 37

Extraction de certificats et de clés privées 38

3 Déploiement du dispositif vRealize Automation 40

À propos du déploiement du dispositif 40

Déployer le dispositif vRealize Automation	40
Ajouter des contrôleurs d'Interface réseau avant d'exécuter le programme d'installation	44

4 Installation avec l'assistant d'installation 46

Utilisation de l'assistant d'installation pour des déploiements minimaux	46
Démarrer l'assistant d'installation pour un déploiement minimal	47
Installer l'agent de gestion	47
Exécution de l'assistant d'installation	49
Utilisation de l'assistant d'installation pour les déploiements d'entreprise	50
Démarrer l'assistant d'installation pour un déploiement d'entreprise	50
Installer l'agent de gestion	51
Exécution de l'assistant d'installation	53

5 Les interfaces d'installation standard 54

Utilisation des interfaces standard pour des déploiements minimaux	55
Liste de contrôle pour un déploiement minimal	55
Configurer le dispositif vRealize Automation	55
Installation des composants IaaS	59
Utilisation des interfaces standard pour les déploiements distribués	66
Liste de contrôle d'un déploiement distribué	66
Désactivation des contrôles de santé de l'équilibrage de charge	68
Exigences de confiance du certificat dans un déploiement distribué	68
Configurer une approbation de certificat pour des hôtes de composants Web, Manager Service et DEM	70
Feuilles d'activité d'installation	71
Configuration de votre équilibrage de charge	74
Configuration de dispositifs pour vRealize Automation	75
Installer les composants IaaS dans une configuration distribuée	82
Installation d'agents	114
Définir la stratégie d'exécution PowerShell sur RemoteSigned	115
Choisir le scénario d'installation de l'agent	115
Emplacement et conditions d'installation de l'agent	116
Installation et configuration de l'agent Proxy pour vSphere	116
Installation de l'agent Proxy pour Hyper-V ou XenServer	123
Installation de l'agent VDI pour XenDesktop	128
Installation de l'agent EPI pour Citrix	132
Installation de l'agent EPI pour les scripts Visual Basic	136
Installation de l'agent WMI pour les demandes WMI à distance	140

6 Installation silencieuse 143

À propos de l'installation silencieuse	143
Effectuer une installation silencieuse	144

Effectuer une installation silencieuse de l'agent de gestion	144
Fichier de réponses pour installation silencieuse	146
La ligne de commande d'installation	147
Notions de base sur l'installation depuis la ligne de commande	147
Noms des commandes d'installation	148
API d'installation	148
Convertir entre propriétés silencieuses et JSON	150

7 Tâches post-installation 152

Ne pas modifier le fuseau horaire	152
Configurer le chiffrement conforme à norme FIPS	153
Activer le basculement automatique de Manager Service	154
À propos du basculement automatique de Manager Service	154
Basculement de la base de données PostgreSQL automatique	155
Remplacement de certificats autosignés par des certificats fournis par une autorité	156
Modification de noms d'hôtes et d'adresses IP	156
Modifier le nom d'hôte du dispositif	156
Modifier l'adresse IP du dispositif	157
Ajuster la base de données SQL pour un nom d'hôte modifié	159
Modifier l'adresse IP d'un serveur IaaS	159
Modifier un nom d'hôte de serveur IaaS	161
Définir l'URL de connexion sur un nom personnalisé	163
Supprimer un nœud du dispositif vRealize Automation	164
Installation de l'agent vRealize Log Insight	164
Modifier le port de proxy de VMware Remote Console	164
Modifier un nom de domaine complet du dispositif et lui attribuer le nom de domaine complet d'origine	165
Configurer le groupe de disponibilité AlwaysOn SQL	166
Ajouter des contrôleurs d'interface réseau après l'installation de vRealize Automation	166
Configurer des routes statiques	168
Gestion des correctifs accès	169
Configurer l'accès au locataire par défaut	170

8 Dépannage d'une installation 172

Emplacement des journaux par défaut	172
Restauration d'une installation qui a échoué	174
Restaurer une installation minimale	174
Restaurer une installation distribuée	175
Créer un bundle de support	176
Dépannage de l'installation générale	177
L'installation des mises à niveau échoue avec une erreur de délai d'attente des équilibrages de charge	177

Les heures des serveurs ne sont pas synchronisées	177
Des pages blanches peuvent apparaître lors de l'utilisation d'Internet Explorer 9 ou 10 sur Windows 7	178
Impossible d'établir une relation de confiance pour le canal sécurisé SSL/TLS	179
Se connecter au réseau par le biais d'un serveur proxy	179
Étapes sur la console pour une configuration de contenu initial	180
Impossible de rétrograder les licences de vRealize Automation	181
Dépannage du dispositif vRealize Automation	182
Le téléchargement des programmes d'installation échoue	182
Le fichier Encryption.key comporte des autorisations incorrectes	182
Échec du démarrage d'Identity Manager pour la gestion des annuaires après le redémarrage de Horizon-Workspace	183
Attributions de rôles de dispositifs incorrectes après basculement	185
Pannes après la promotion de nœuds de réplica et master	186
Enregistrements des services composants incorrects	186
La carte réseau supplémentaire provoque des erreurs d'interface de gestion	189
Impossible de promouvoir un dispositif virtuel secondaire au rang de dispositif master	189
La durée de rétention du journal de synchronisation Active Directory est trop courte	190
RabbitMQ ne parvient pas à résoudre les noms d'hôte	191
Dépannage des composants IaaS	192
Les connexions du coordinateur de transaction distribué sont refusées	192
Le programme de correction des conditions préalables ne peut pas installer les fonctionnalités .NET	192
Validation des certificats de serveur pour IaaS	193
Erreur d'informations d'identification lors de l'exécution du programme d'installation d'IaaS	194
Un avertissement d'enregistrement des paramètres s'affiche lors de l'installation d'IaaS	194
Échec de l'installation du serveur de site Web et des Distributed Execution Managers	195
L'authentification IaaS échoue lors de l'installation d'IaaS Web et de Model Management	195
L'installation des données Model Manager et des composants Web a échoué	196
Les serveurs Windows IaaS ne prennent pas en charge la norme FIPS	197
L'ajout d'un point de terminaison XaaS génère une erreur interne	198
Échec de la désinstallation de l'agent proxy	198
Les demandes de machine échouent lorsque les transactions à distance sont désactivées	199
Erreur dans la communication de Manager Service	200
Le comportement de personnalisation des e-mails a été modifié	201
Dépannage des erreurs de connexion	202
Des tentatives de connexion en tant qu'administrateur IaaS avec des informations d'identification au format UPN incorrect échouent sans explication	202
La connexion échoue avec la haute disponibilité	202
Le proxy empêche l'utilisateur de VMware Identity Manager de se connecter	203

Installation de vRealize Automation

Ce guide d'*Installation vRealize Automation* contient des instructions d'installation en mode silencieux, manuelle et avec assistant pour VMware vRealize™ Automation.

Note Toutes les fonctionnalités et capacités de vRealize Automation sont disponibles dans toutes les éditions. Pour obtenir un comparatif des ensembles de fonctionnalités de chaque édition, reportez-vous à <https://www.vmware.com/products/vrealize-automation/>.

Public visé

Ces informations s'adressent à des administrateurs de systèmes Windows ou Linux qui connaissent la technologie des machines virtuelles et le fonctionnement des centres de données.

Informations mises à jour

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

Révision	Description
XX À DÉTERMINER 202X	<ul style="list-style-type: none">■ Mise à jour de Installer l'agent de gestion vRealize Automation.■ Mise à jour de Activer le basculement automatique de Manager Service.■ Mise à jour de Création d'un bundle de support vRealize Automation.■ Mise à jour de Enregistrements des services composants vRealize Automation incorrects.
12 août 2020	Mise à jour de Extraction de certificats et de clés privées .
14 février 2020	<ul style="list-style-type: none">■ Mise à jour de Serveurs Windows IaaS.■ Mise à jour de Hôte Manager Service IaaS.■ Mise à jour de Hôte du serveur SQL IaaS.■ Mise à jour de Ne pas modifier le fuseau horaire vRealize Automation.■ Mise à jour de Gestion des correctifs accès.■ Ajout de Les connexions du coordinateur de transaction distribué sont refusées.■ Mise à jour de Les demandes de machine échouent lorsque les transactions à distance sont désactivées.
24 octobre 2019	Ajout du rappel de connecteur à Ajouter un autre dispositif vRealize Automation au cluster .
9 septembre 2019	Ajout de Ne pas modifier le fuseau horaire vRealize Automation .
14 juin 2019	<ul style="list-style-type: none">■ Paramètres de stratégie de groupe mis à jour dans Comptes et mots de passe.■ Paramètres régionaux anglais mis à jour dans Serveurs Windows IaaS.
30 mai 2019	<ul style="list-style-type: none">■ Paramètres de stratégie de groupe ajoutés dans Comptes et mots de passe.■ Suppression de PowerShell 2 et ajout des paramètres régionaux anglais dans Serveurs Windows IaaS.
7 mai 2019	Correction de plusieurs liens hypertextes.
1er mars 2019	Liens LCM ajoutés dans À propos de l'installation de vRealize Automation .
12 février 2019	Mise à jour de l'exigence de la version 1.8, Update 181 ou version ultérieure de Java.
13 novembre 2018	Ajout de SQL Server 2017

Révision	Description
4 octobre 2018	<ul style="list-style-type: none">■ Ajout d'une référence aux spécifications matérielles accrues dans la section Hôte du serveur SQL IaaS.■ Ajout du lien vers l'article de la base de connaissances sur le délai d'expiration dans la section Ajouter un autre dispositif vRealize Automation au cluster.■ Ajout des conditions préalable en matière de nom de domaine complet du certificat dans les sections Installer des composants de serveur Web IaaS supplémentaires et Installer un composant de sauvegarde Manager Service.■ Modification du lien vers un article de la Base de connaissances dans la section Supprimer un nœud du dispositif vRealize Automation.■ Ajout du problème de clé de base de données dans l'aide en ligne.
20 septembre 2018	Version de document initiale.

Présentation de l'installation de vRealize Automation

1

Vous pouvez installer vRealize Automation pour prendre en charge des environnements de validation technique minimaux, ou dans différentes tailles de configurations d'entreprise distribuées, qui sont capables de gérer des charges de travail de production. L'installation peut être interactive ou silencieuse.

Après l'installation, vous commencez à utiliser vRealize Automation en personnalisant votre installation et en configurant des locataires, ce qui fournit aux utilisateurs un accès au provisionnement en libre-service et à la gestion du cycle de vie des services cloud.

Ce chapitre contient les rubriques suivantes :

- [À propos de l'installation de vRealize Automation](#)
- [Nouveautés dans cette installation vRealize Automation](#)
- [Composants d'installation de vRealize Automation](#)
- [Type de déploiement](#)
- [Choisir votre méthode d'installation](#)

À propos de l'installation de vRealize Automation

Vous pouvez installer vRealize Automation par d'autres moyens, chacun offrant des niveaux variables d'interactivité.

Pour procéder à l'installation, vous déployez un dispositif vRealize Automation, puis vous complétez l'installation en utilisant l'une des options suivantes :

- Assistant d'installation consolidée basée sur un navigateur
- Configuration distincte de dispositifs basée sur un navigateur et installations Windows distinctes pour des composants de serveur IaaS
- Programme d'installation silencieux basé sur une ligne de commande qui accepte une entrée provenant d'un fichier de propriétés de réponse
- API REST d'installation qui accepte une entrée au format JSON

Vous pouvez également installer vRealize Automation à l'aide de Lifecycle Manager. Pour plus d'informations, reportez-vous au [Guide d'installation, de mise à niveau et de gestion de vRealize Suite Lifecycle Manager](#).

vRealize Suite Lifecycle Manager automatise l'installation, la configuration, la mise à niveau, la correction, la gestion de la configuration, la correction de la dérive et la santé depuis un écran unique. Cliquez ici pour installer [vRealize Suite Lifecycle Manager](#). Lifecycle Manager permet aux responsables informatiques des ressources d'administration cloud de se concentrer sur les initiatives stratégiques tout en améliorant le retour sur investissement, la fiabilité et la cohérence.

Nouveautés dans cette installation vRealize Automation

Si vous avez installé des versions antérieures de vRealize Automation, soyez attentif aux changements dans le processus d'installation de cette version.

L'interface d'administration du dispositif vRealize Automation a changé.

- Les fonctions de l'onglet Base de données ont été déplacées dans l'onglet Cluster. L'onglet Base de données a été supprimé et l'onglet Cluster est devenu un onglet principal.
- L'onglet Migration est devenu un onglet principal et comprend maintenant vRealize Automation et vRealize Orchestrator.
- L'option de bundle de support est passée à l'onglet Journaux.
- vRealize Code Stream a été supprimé à partir de l'onglet Licences.

Composants d'installation de vRealize Automation

Une installation vRealize Automation typique est composée d'un dispositif vRealize Automation et d'un ou plusieurs serveurs Windows qui ensemble fournissent l'infrastructure vRealize Automation comme un service (IaaS).

Le dispositif vRealize Automation

Le dispositif vRealize Automation est un dispositif virtuel Linux préconfiguré. Le dispositif vRealize Automation est livré en tant que fichier de virtualisation ouvert que vous pouvez déployer sur une infrastructure virtualisée existante telle que vSphere.

Le dispositif vRealize Automation exécute plusieurs fonctions essentielles de vRealize Automation.

- Le dispositif contient le serveur qui héberge le portail du produit vRealize Automation, dans lequel les utilisateurs se connectent pour accéder au provisionnement en libre-service et à la gestion des services cloud.
- Le dispositif gère Single Sign-On (SSO) pour l'autorisation et l'authentification des utilisateurs.
- Le serveur de dispositifs héberge une interface de gestion pour les paramètres du dispositif vRealize Automation.

- Le dispositif inclut une base de données PostgreSQL préconfigurée utilisée pour les opérations internes du dispositif vRealize Automation.

Dans les grands déploiements comportant des dispositifs redondants, les bases de données de dispositifs secondaires servent de réplicas pour assurer une haute disponibilité.

- Le dispositif inclut une instance préconfigurée de vRealize Orchestrator. vRealize Automation utilise des workflows et des actions vRealize Orchestrator pour étendre ses fonctionnalités.

L'instance intégrée de vRealize Orchestrator est maintenant recommandée. Dans les anciens déploiements ainsi que dans certains cas particuliers, les utilisateurs pouvaient plutôt connecter vRealize Automation à une instance externe de vRealize Orchestrator.

- Le dispositif contient le programme d'installation téléchargeable de l'agent de gestion. Tous les serveurs Windows qui composent votre instance de vRealize Automation IaaS doivent installer l'agent de gestion.

L'agent de gestion enregistre les serveurs Windows IaaS dans le dispositif vRealize Automation, automatise l'installation et la gestion des composants IaaS et collecte des informations de support et de télémétrie.

IaaS (Infrastructure en tant que service)

vRealize Automation IaaS est composé d'un ou de plusieurs serveurs Windows qui collaborent pour modéliser et provisionner des systèmes dans des infrastructures cloud privées, publiques ou hybrides.

Vous installez des composants vRealize Automation IaaS sur un ou plusieurs serveurs Windows virtuels ou physiques. Après l'installation, les opérations IaaS figurent sous l'onglet Infrastructure dans l'interface du produit.

IaaS est composé des composants suivants, qui peuvent être installés ensemble ou séparément, selon la taille du déploiement.

Serveur Web

Le serveur Web IaaS assure l'administration de l'infrastructure et la création de services dans l'interface du produit vRealize Automation. Le composant du serveur Web communique avec Manager Service, qui fournit des mises à jour à partir de Distributed Execution Manager (DEM), la base de données SQL Server et des agents.

Model Manager

vRealize Automation utilise des modèles pour faciliter l'intégration à des systèmes et des bases de données externes. Les modèles mettent en œuvre la logique métier utilisée par le DEM.

Model Manager fournit des services et des utilitaires pour les éléments du modèle de persistance, de contrôle de version, de sécurisation et de distribution. Model Manager est hébergé sur l'un des serveurs Web IaaS et communique avec les DEM, la base de données SQL Server et le site Web de l'interface du produit.

Manager Service

Le composant Manager Service est un service Windows qui coordonne la communication entre les DEM IaaS, la base de données SQL Server, les agents et SMTP. En outre, le composant Manager Service communique avec le serveur Web par le biais de Model Manager et doit s'exécuter sous un compte de domaine avec des privilèges d'administrateur local sur tous les serveurs IaaS Windows.

Sauf si vous activez le basculement automatique de Manager Service, IaaS impose qu'une seule machine Windows à la fois exécute de façon active le composant Manager Service. Pour la sauvegarde ou la haute disponibilité, vous pouvez déployer des machines Manager Service supplémentaires, mais l'approche de basculement manuel impose que le service soit arrêté et configuré pour démarrer manuellement sur les machines de sauvegarde.

Pour plus d'informations, reportez-vous à [À propos du basculement automatique de Manager Service](#).

Base de données SQL Server

IaaS utilise une base de données Microsoft SQL Server pour mettre à jour les informations sur les machines qu'il gère, ainsi que ses propres éléments et stratégies. La plupart des utilisateurs autorisent vRealize Automation à créer la base de données pendant l'installation. Vous pouvez également créer la base de données séparément en fonction de vos stratégies.

Distributed Execution Manager

Le composant DEM IaaS exécute la logique métier de modèles personnalisés, interagissant avec la base de données SQL Server IaaS, ainsi qu'avec des bases de données et des systèmes externes. Une approche fréquente consiste à installer des composants DEM sur le serveur IaaS Windows qui héberge le composant Manager Service actif, mais n'est pas obligatoire.

Chaque instance du composant DEM agit comme un worker ou un orchestrateur. Les rôles peuvent être installés sur le même serveur ou sur des serveurs distincts.

Service DEM Worker—Un service DEM a une fonction, exécuter des workflows. Plusieurs services DEM Worker augmentent la capacité et peuvent être installés sur le même serveur ou sur des serveurs distincts.

DEM Orchestrator—Un composant DEM Orchestrator effectue les fonctions de surveillance suivantes.

- Surveille les composants DEM Worker. Si un composant Worker s'arrête ou perd sa connexion à Model Manager, le composant DEM Orchestrator déplace les workflows vers un autre composant DEM Worker.
- Planifie les workflows en créant des instances de workflow au moment planifié.
- Vérifie qu'une seule instance d'un workflow planifié est exécutée à un moment donné.
- Prétraite les workflows avant qu'ils ne s'exécutent. Le prétraitement inclut la vérification de préconditions pour les workflows et la création de l'historique d'exécution des workflows.

Le composant DEM Orchestrator actif a besoin d'une solide connexion réseau à l'hôte Model Manager. Dans les grands déploiements à plusieurs composants DEM Orchestrator sur des serveurs distincts, les orchestrateurs secondaires servent de sauvegardes. Les composants DEM Orchestrator secondaires surveillent le composant DEM orchestrator actif et fournissent la redondance et le basculement en cas de problème avec le composant DEM orchestrator actif. Pour ce type de configuration de basculement, vous pouvez envisager d'installer le composant DEM Orchestrator actif avec l'hôte Manager Service actif, et les composants DEM Orchestrator secondaires avec les hôtes Manager Service en attente.

Agents

vRealize Automation IaaS utilise des agents pour s'intégrer à des systèmes externes et gérer des informations parmi les composants vRealize Automation.

Une approche fréquente consiste à installer des agents vRealize Automation sur le serveur IaaS Windows qui héberge le composant Manager Service actif, mais n'est pas obligatoire. Plusieurs agents augmentent la capacité et peuvent être installés sur le même serveur ou sur des serveurs distincts.

Agents proxy de virtualisation

vRealize Automation crée et gère des machines virtuelles sur des hôtes de virtualisation. Les agents proxy de virtualisation envoient des commandes à vSphere ESX Server, XenServer, à des hôtes Hyper-V et aux machines virtuelles qui y sont provisionnées, et y collectent des données.

Un agent proxy de virtualisation a les caractéristiques suivantes.

- Il nécessite généralement des privilèges d'administrateur sur la plate-forme de virtualisation qu'il gère.
- Il communique avec Manager Service IaaS.
- Il est installé séparément et dispose de son propre fichier de configuration.

La plupart des déploiements vRealize Automation installent l'agent proxy vSphere. Vous pouvez installer d'autres agents proxy selon les ressources de virtualisation utilisées sur votre site.

Agents Virtual Desktop Integration (VDI)

Les agents Virtual desktop integration (VDI) PowerShell permettent à vRealize Automation de s'intégrer à des systèmes externes de bureau virtuel. Les agents VDI nécessitent des privilèges d'administrateur sur les systèmes externes.

Vous pouvez enregistrer des machines virtuelles provisionnées par vRealize Automation avec sur un contrôleur DDC (Desktop Delivery Controller) Citrix, qui permet à l'utilisateur d'accéder à l'interface Web de XenDesktop à partir de vRealize Automation.

Agents External Provisioning Integration (EPI)

Les agents External provisioning integration (EPI) PowerShell permettent à vRealize Automation de s'intégrer à des systèmes externes dans le processus de provisionnement de la machine.

Par exemple, l'intégration au serveur de provisionnement Citrix permet de provisionner des machines via la diffusion de disques à la demande et les agents EPI vous permettent d'exécuter des scripts Visual Basic en tant qu'étapes supplémentaires dans le processus de provisionnement.

Les agents EPI nécessitent des privilèges d'administrateur sur les systèmes externes avec lesquels ils interagissent.

Agent Windows Management Instrumentation

L'agent vRealize Automation Windows Management Instrumentation (WMI) améliore votre capacité à surveiller et à contrôler les informations système et vous permet de gérer des serveurs Windows distants depuis un emplacement central. L'agent WMI permet également la collecte de données à partir de serveurs Windows gérés par vRealize Automation.

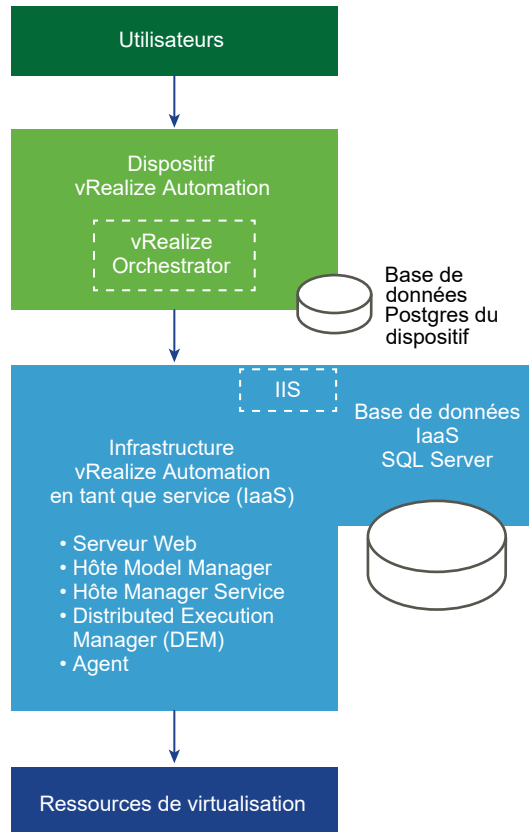
Type de déploiement

Vous pouvez installer vRealize Automation en tant que déploiement minimal pour validation technique ou travail de développement, ou dans une configuration distribuée adaptée à des charges de travail de production de taille moyenne à grande.

Déploiements vRealize Automation minimaux

Les déploiements minimaux incluent un dispositif vRealize Automation et un serveur Windows qui héberge les composants IaaS. Dans un déploiement minimal, la base de données vRealize Automation SQL Server peut se trouver sur le même serveur Windows IaaS avec les composants IaaS, ou sur un serveur Windows distinct.

Figure 1-1. Déploiement vRealize Automation minimal

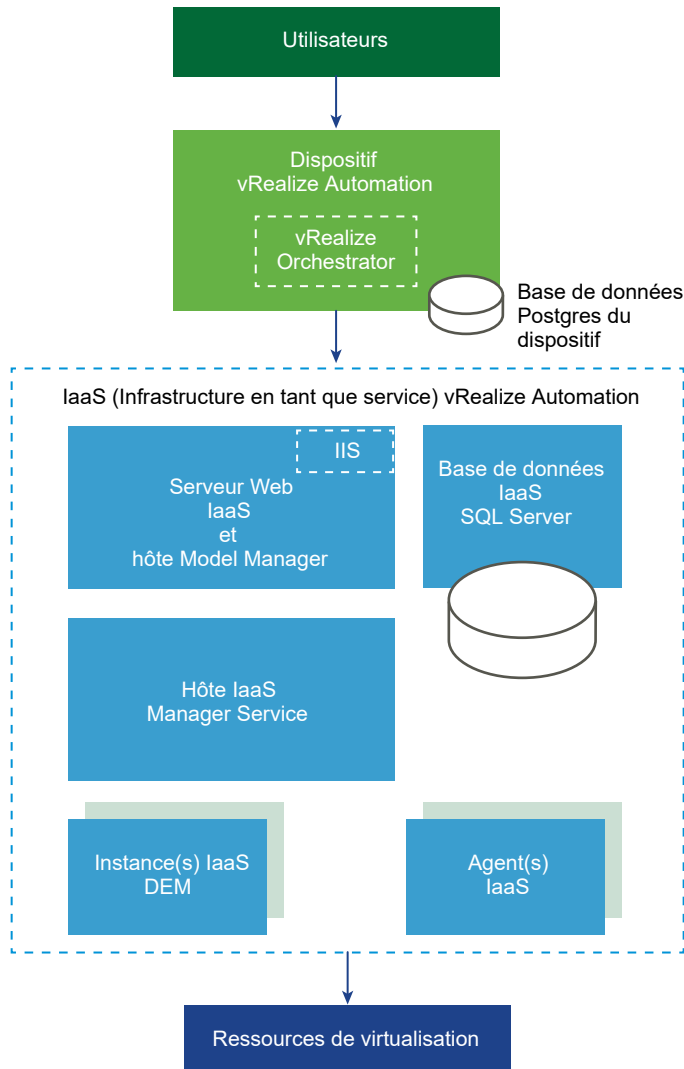


Vous ne pouvez pas convertir un déploiement minimal en un déploiement d'entreprise. Pour monter un déploiement en puissance, commencez par un déploiement de petite entreprise, puis ajoutez-y des composants. Il n'est pas possible de commencer avec un déploiement minimal.

Déploiements vRealize Automation distribués

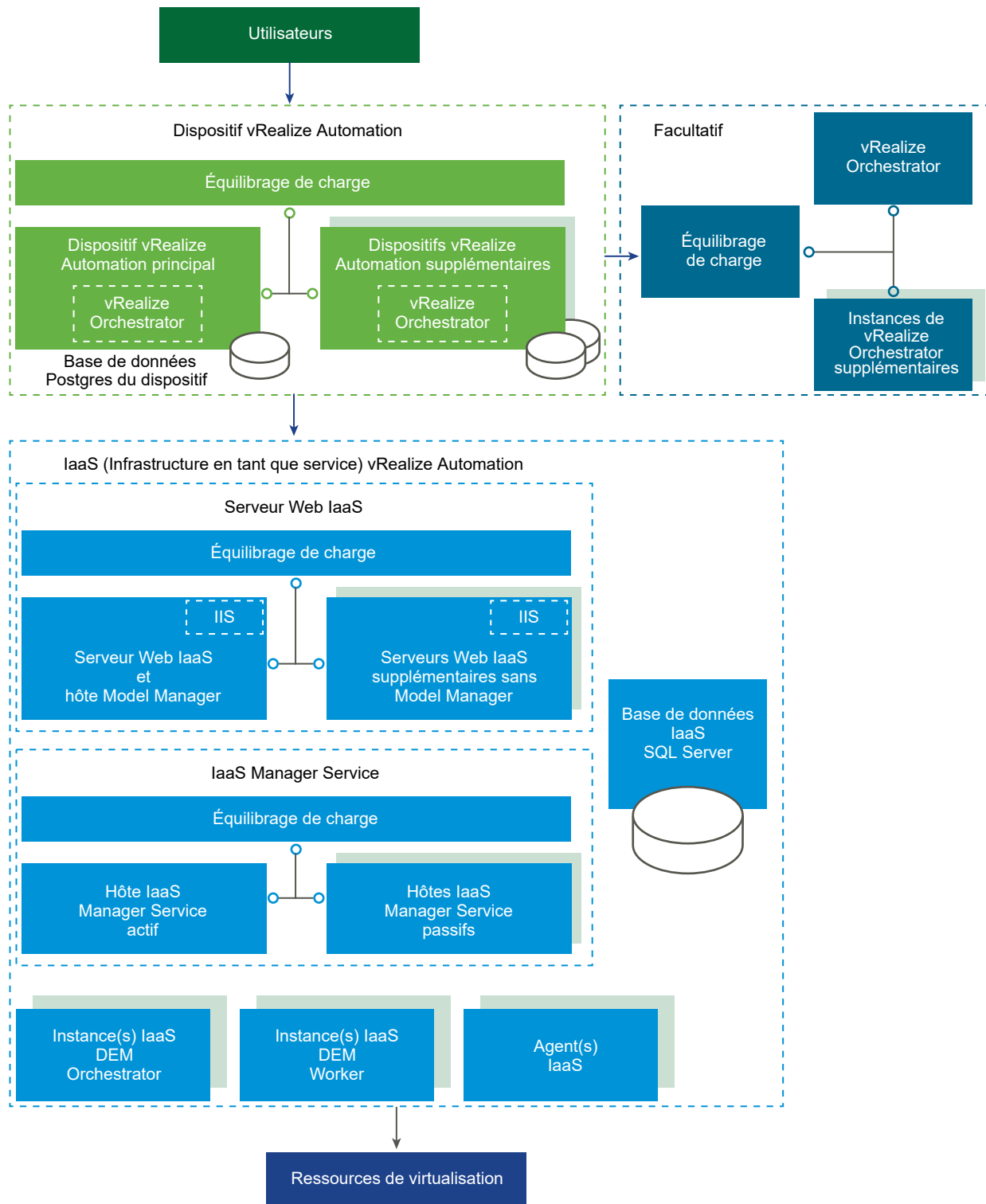
Les déploiements distribués d'entreprise peuvent avoir des tailles variables. Un déploiement distribué de base peut améliorer vRealize Automation simplement en hébergeant les composants IaaS sur des serveurs Windows distincts comme le montre la figure suivante.

Figure 1-2. Déploiement vRealize Automation distribué



De nombreux déploiements de production vont même plus loin, avec des dispositifs redondants, des serveurs redondants et un équilibrage de charge pour offrir une capacité encore supérieure. Les grands déploiements distribués offrent une meilleure échelle, une haute disponibilité et une récupération d'urgence. Notez que l'instance intégrée de vRealize Orchestrator est maintenant recommandée, mais vous pouvez voir vRealize Automation connecté à une instance externe de vRealize Orchestrator dans d'anciens déploiements.

Figure 1-3. Déploiement vRealize Automation distribué et faisant l'objet d'un équilibrage de charge



Pour obtenir des informations sur l'évolutivité et la haute disponibilité, reportez-vous au guide *d'architecture de référence de vRealize Automation*.

Choisir votre méthode d'installation

L'assistant d'installation consolidée de vRealize Automation est votre principal outil pour de nouvelles installations vRealize Automation. Sinon, vous voulez peut-être effectuer des processus d'installation manuels et distincts ou une installation silencieuse.

- L'assistant d'installation offre une façon simple et rapide d'effectuer une installation, des déploiements minimaux aux déploiement d'entreprise distribués, avec ou sans équilibrage de charge. La plupart des utilisateurs exécutent l'assistant installation.
- Si vous souhaitez étendre un déploiement vRealize Automation ou si l'assistant d'installation s'est arrêté pour une raison quelconque, les étapes d'installation manuelle vous seront utiles. Une fois que vous avez commencé une installation manuelle, vous ne pouvez pas revenir en arrière et exécuter l'assistant d'installation.
- En fonction des besoins de votre site, vous pourrez également bénéficier d'une installation de ligne de commande ou d'installation basée sur une API en mode silencieux.

Préparation à l'installation de vRealize Automation

2

Vous installez vRealize Automation dans l'infrastructure de virtualisation existante. Avant de commencer une installation, vous devez satisfaire à certaines conditions requises du système et de l'environnement.

Ce chapitre contient les rubriques suivantes :

- [Préparation générale](#)
- [Comptes et mots de passe](#)
- [Noms d'hôtes et adresses IP](#)
- [Latence et bande passante](#)
- [Dispositif vRealize Automation](#)
- [Serveurs Windows IaaS](#)
- [Serveur Web IaaS](#)
- [Hôte Manager Service IaaS](#)
- [Hôte du serveur SQL IaaS](#)
- [Hôte DEM \(Distributed Execution Manager\) IaaS](#)
- [Certificats](#)

Préparation générale

Plusieurs éléments doivent être pris en compte à l'échelle du déploiement avant d'installer vRealize Automation.

Pour en savoir plus sur les conditions requises de haut niveau pour l'environnement, notamment les versions de navigateur et de système d'exploitation prises en charge, consultez la [Matrice de support de vRealize Automation](#).

Navigateurs Web utilisateur

Les fenêtres et onglets de navigateur multiples ne sont pas pris en charge. vRealize Automation prend en charge une session par utilisateur.

Les consoles VMware distantes provisionnées sur vSphere prennent uniquement en charge un sous-ensemble de navigateurs vRealize Automation pris en charge.

Logiciels tiers

Tous les logiciels tiers doivent disposer des derniers correctifs du fournisseur. Les logiciels tiers incluent Microsoft Windows et SQL Server.

Synchronisation de l'heure

Tous les dispositifs vRealize Automation et serveurs Windows IaaS doivent se synchroniser avec la même source de temps. Vous ne pouvez utiliser que l'une des sources suivantes. Ne mélangez pas les sources de temps.

- L'hôte du dispositif vRealize Automation
- Un serveur NTP (Network Time Protocol) externe

Pour utiliser l'hôte du dispositif vRealize Automation, vous devez exécuter NTP sur l'hôte ESXi. Pour en savoir plus sur le chronométrage, consultez [Article 1318 de la base de connaissances VMware](#).

Vous sélectionnez la source de temps sur la page Conditions préalables d'installation de l'assistant d'installation.

Comptes et mots de passe

Vous devrez éventuellement créer plusieurs comptes d'utilisateurs et mots de passe ou planifier les paramètres pour ceux-ci avant d'installer vRealize Automation.

Compte de service IaaS

IaaS installe plusieurs services Windows qui doivent s'exécuter sous un compte d'utilisateur unique.

- Le compte doit être un utilisateur de domaine.
- Le compte ne doit pas nécessairement être un administrateur de domaine, mais il doit disposer des autorisations d'administrateur local, avant l'installation, sur tous les serveurs Windows IaaS.
- Le mot de passe du compte ne peut pas contenir de caractère guillemet double (").
- Le programme d'installation de l'agent de gestion pour les serveurs Windows IaaS vous invite à entrer les informations d'identification du compte.
- Le compte doit disposer de l'autorisation **Ouverture de session en tant que service**, ce qui permet à Manager Service de démarrer et de générer des fichiers journaux.
- Le compte doit disposer de l'autorisation dbo sur la base de données IaaS.

Si vous utilisez le programme d'installation pour créer la base de données, ajoutez la connexion au compte à SQL Server avant l'installation. Le programme d'installation octroie l'autorisation dbo après avoir créé la base de données.

- Si vous utilisez le programme d'installation pour créer la base de données, dans SQL ajoutez le rôle sysadmin au compte avant l'installation.

Le rôle sysadmin n'est pas requis si vous choisissez d'utiliser une base de données vide préexistante.

- Si votre site utilise des paramètres de sécurité de stratégie de groupe, vérifiez les paramètres suivants pour le compte. Exécutez l'éditeur de stratégie de groupe gpedit.msc et regardez sous **Configuration d'ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur**.
 - Refuser la connexion localement—Ne pas ajouter le compte.
 - Autoriser la connexion localement—Ajouter le compte.
 - Refuser l'accès à cet ordinateur à partir du réseau—Ne pas ajouter le compte.
 - Accéder à cet ordinateur à partir du réseau—Ajouter le compte.

Identité de pool d'applications IIS

Le compte que vous utilisez en tant qu'identité de pool d'applications IIS pour le service Web Model Manager doit avoir l'autorisation **Ouverture de session en tant que travail par lot**.

Informations d'identification de base de données IaaS

Vous pouvez laisser le programme d'installation de vRealize Automation créer la base de données ou vous pouvez la créer séparément à l'aide de SQL Server. Lorsque le programme d'installation de vRealize Automation crée la base de données, les conditions requises suivantes s'appliquent.

- Pour le programme d'installation de vRealize Automation, si vous sélectionnez l'authentification Windows, le compte qui exécute l'agent de gestion sur le serveur Web IaaS principal doit avoir le rôle sysadmin dans SQL pour créer la base de données et en modifier la taille.
- Pour le programme d'installation de vRealize Automation, même si vous ne sélectionnez pas l'authentification Windows, le compte qui exécute l'agent de gestion sur le serveur Web IaaS principal doit avoir le rôle sysadmin dans SQL, car les informations d'identification sont utilisées au moment de l'exécution.
- Si vous créez séparément la base de données, les informations d'identification de l'utilisateur Windows ou de l'utilisateur SQL que vous fournissez nécessitent uniquement l'autorisation dbo sur la base de données.

Phrase secrète de sécurité de la base de données IaaS

La phrase secrète de sécurité de la base de données génère une clé de chiffrement qui protège les données dans la base de données SQL IaaS. Vous spécifiez la phrase secrète de sécurité sur la page Hôte IaaS de l'assistant d'installation.

- Prévoyez d'utiliser la même phrase secrète de sécurité de base de données dans toute l'installation afin que chaque composant dispose de la même clé de chiffrement.
- Enregistrez la phrase secrète, car vous en aurez besoin pour restaurer la base de données en cas de panne ou pour ajouter des composants après l'installation initiale.
- La phrase secrète de sécurité de base de données ne peut pas contenir de caractère guillemet double ("). La phrase secrète est acceptée lors de sa création, mais entraîne l'échec de l'installation.

Points de terminaison vSphere

Si vous prévoyez un provisionnement sur un point de terminaison vSphere, vous avez besoin d'un compte de domaine ou d'un compte local avec des autorisations suffisantes pour effectuer des opérations sur la cible. Le niveau d'autorisation approprié doit également être configuré pour le compte dans vRealize Orchestrator.

Mot de passe d'administrateur de vRealize Automation

Après l'installation, le mot de passe d'administrateur de vRealize Automation vous connecte au locataire par défaut. Vous spécifiez le mot de passe de l'administrateur sur la page Single Sign-On de l'assistant d'installation.

Le mot de passe de l'administrateur vRealize Automation ne peut pas contenir de caractère (=) de fin. Le mot de passe est accepté lors de sa création mais entraîne des erreurs lorsque vous effectuez des opérations comme l'enregistrement de points de terminaison.

Noms d'hôtes et adresses IP

vRealize Automation impose que vous nommiez les hôtes dans votre installation en respectant certaines conditions.

- Toutes les machines vRealize Automation de votre installation doivent pouvoir se résoudre entre elles par des noms de domaine complets.

Au moment de l'installation, entrez toujours le nom de domaine complet lors de l'identification ou de la sélection d'une machine vRealize Automation. N'entrez pas d'adresses IP ou de noms de machine courts.

- Outre la condition requise du nom de domaine complet, les machines Windows qui hébergent le service Web Model Manager, Manager Service et la base de données Microsoft SQL Server doivent pouvoir se résoudre mutuellement par le nom du service WINS (Windows Internet Name Service).

Configurez votre nom DNS (Domain Name System) de manière à résoudre ces noms d'hôtes WINS courts.

- Planifiez la dénomination des domaines et des machines afin que les noms de machine vRealize Automation commencent par une lettre (a-z, A-Z), se terminent par une lettre ou un chiffre (0 à 9), et que seuls des lettres, des chiffres ou des traits d'union (-) figurent au milieu. Le caractère tiret de soulignement (_) ne doit pas figurer dans le nom d'hôte ou dans le nom de domaine complet.

Pour plus d'informations sur les noms autorisés, lisez les spécifications de noms d'hôtes du groupe de travail IETF (Internet Engineering Task Force). Reportez-vous à www.ietf.org.

- En général, il convient de conserver les noms d'hôtes et les noms de domaine que vous prévoyez d'utiliser pour les systèmes vRealize Automation. La modification d'un nom d'hôte n'est pas toujours possible. Quand une modification est possible, la procédure peut être complexe.
- Il est recommandé de réserver et d'utiliser des adresses IP statiques pour tous les dispositifs vRealize Automation et pour les serveurs IaaS Windows. vRealize Automation prend en charge DHCP, mais des adresses IP statiques sont recommandées pour des déploiements à long terme tels que des environnements de production.
 - Vous appliquez une adresse IP au dispositif vRealize Automation pendant un déploiement OVF ou OVA.
 - Pour les serveurs IaaS Windows, vous suivez le processus habituel du système d'exploitation. Définissez l'adresse IP avant d'installer vRealize Automation IaaS.

Latence et bande passante

vRealize Automation prend en charge l'installation distribuée sur plusieurs sites, mais la vitesse et le volume de transmission des données doivent satisfaire aux conditions minimales requises.

vRealize Automation nécessite un environnement d'une latence réseau de 5 ms ou moins, et d'une bande passante de 1 Go ou plus, parmi les composants suivants.

- Dispositif vRealize Automation
- Serveur Web IaaS
- Hôte Model Manager IaaS
- Hôte Manager Service IaaS
- Base de données SQL Server IaaS
- DEM Orchestrator IaaS

Le composant suivant peut fonctionner sur un site de latence plus élevée, mais la pratique n'est pas recommandée.

- DEM Worker IaaS

Vous pouvez installer le composant suivant à l'emplacement du point de terminaison avec lequel il communique.

- Agent proxy IaaS

Dispositif vRealize Automation

La plupart des conditions requises du dispositif vRealize Automation sont préconfigurées dans le fichier OVF ou OVA que vous déployez. Les mêmes conditions requises s'appliquent à des dispositifs vRealize Automation autonomes, master ou réplicas.

Le matériel de machine virtuelle minimal sur lequel vous pouvez effectuer un déploiement est la version 7, ESX/ESXi 4.x ou une version ultérieure. Reportez-vous à [Article 2007240 de la base de connaissances VMware](#). En raison de la demande de ressources matérielles, n'effectuez pas de déploiement sur VMware Workstation.

VMware ne prend pas en charge les modifications ou les personnalisations de dispositif. Ne jamais ajouter, supprimer ou mettre à jour des modules ou des scripts personnalisés, notamment des logiciels antivirus.

Après le déploiement, vous pouvez utiliser vSphere pour ajuster les paramètres matériels du dispositif vRealize Automation pour satisfaire aux conditions requises d'Active Directory. Consultez le tableau suivant.

Tableau 2-1. Conditions matérielles requises du dispositif vRealize Automation pour Active Directory

Dispositif vRealize Automation pour les petits annuaires Active Directory	Dispositif vRealize Automation pour les grands annuaires Active Directory
<ul style="list-style-type: none"> ■ 4 CPU ■ 18 Go de mémoire ■ 60 Go de stockage sur disque 	<ul style="list-style-type: none"> ■ 4 CPU ■ 22 Go de mémoire ■ 60 Go de stockage sur disque

Un petit annuaire Active Directory peut contenir jusqu'à 25 000 utilisateurs dans l'unité d'organisation (UO) à synchroniser dans la configuration du magasin d'ID. Un grand annuaire Active Directory peut contenir plus de 25 000 utilisateurs dans l'unité d'organisation.

Ports du dispositif vRealize Automation

Les ports sur le dispositif vRealize Automation sont habituellement préconfigurés dans le fichier OVF ou OVA que vous déployez.

Les ports suivants sont utilisés par le dispositif vRealize Automation.

Tableau 2-2. Ports entrants

Port	Protocole	Commentaires
22	TCP	Facultatif. Accès pour les sessions SSH.
80	TCP	Facultatif. Redirige vers le port 443.

Tableau 2-2. Ports entrants (suite)

Port	Protocole	Commentaires
88	TCP (UDP facultatif)	Authentification Kerberos KDC Cloud à partir de périphériques mobiles externes.
443	TCP	Accès à la console vRealize Automation et aux appels d'API.
		Accès permettant aux machines de télécharger l'agent invité et l'agent de démarrage logiciel.
		Accès pour l'équilibrage de charge et le navigateur.
4369, 5671, 5672, 25672	TCP	Messagerie RabbitMQ.
5480	TCP	Accès à l'interface de gestion du dispositif virtuel.
		Utilisé par l'agent de gestion.
5488, 5489	TCP	Utilisé en interne par le dispositif vRealize Automation pour les mises à jour.
8230, 8280, 8281, 8283	TCP	Instance de vRealize Orchestrator interne.
8443	TCP	Accès pour le navigateur. Port d'administrateur Identity Manager sur HTTPS.
8444	TCP	Communication du proxy de console pour les connexions de VMware Remote Console pour vSphere.
8494	TCP	Synchronisation du cluster de service de conteneur
9300–9400	TCP	Accès pour les audits Identity Manager.
54328	UDP	
40002, 40003	TCP	synchronisation du cluster vIDM
8090, 8092	TCP	Utilisé par le service de santé pour se connecter entre les nœuds vRA

Tableau 2-3. Ports sortants

Port	Protocole	Commentaires
25, 587	TCP, UDP	SMTP pour l'envoi d'un e-mail de notification sortant.
53	TCP, UDP	Serveur DNS.
67, 68, 546, 547	TCP, UDP	DHCP.
80	TCP	Facultatif. Pour extraire des mises à jour logicielles. Les mises à jour peuvent être téléchargées séparément et appliquées.
88, 464, 135	TCP, UDP	Contrôleur de domaine.
110, 995	TCP, UDP	POP pour recevoir un e-mail de notification entrant.
143, 993	TCP, UDP	IMAP pour recevoir un e-mail de notification entrant.

Tableau 2-3. Ports sortants (suite)

Port	Protocole	Commentaires
123	TCP, UDP	Facultatif. Pour la connexion directe au NTP au lieu d'utiliser l'heure de l'hôte.
389	TCP	Accès au serveur de connexion View.
389, 636, 3268, 3269	TCP	Active Directory. Les ports par défaut sont affichés, mais configurables.
443	TCP	Communication avec IaaS Manager Service et les hôtes des points de terminaison de l'infrastructure sur HTTPS.
		Communication avec le service de logiciel vRealize Automation sur HTTPS.
		Accès au serveur de mise à niveau Identity Manager.
		Accès au serveur de connexion View.
445	TCP	Accès au référentiel ThinApp pour Identity Manager.
902	TCP	Opérations de copie de fichiers réseau ESXi et connexions de VMware Remote Console.
5050	TCP	Facultatif. Pour communiquer avec vRealize Business for Cloud.
5432	TCP, UDP	Facultatif. Pour communiquer avec une autre base de données PostgreSQL du dispositif.
5500	TCP	Système RSA SecurID. Le port par défaut est affiché, mais configurable.
8281	TCP	Facultatif. Pour communiquer avec une instance de vRealize Orchestrator externe.
8494	TCP	Synchronisation du cluster de service de conteneur
9300–9400	TCP	Accès pour les audits Identity Manager.
54328	UDP	
40002, 40003	TCP	synchronisation du cluster vIDM

D'autres ports peuvent être requis par des plug-ins vRealize Orchestrator spécifiques communiquant avec des systèmes externes. Pour en savoir plus sur le plug-in vRealize Orchestrator, consultez la documentation.

Serveurs Windows IaaS

Tous les serveurs Windows qui hébergent des composants IaaS doivent satisfaire certaines conditions requises. Traitez les conditions requises avant d'exécuter l'Assistant d'installation vRealize Automation ou le programme d'installation basé sur Windows standard.

Important L'installation désactive le pare-feu Windows. Si des stratégies de site nécessitent le pare-feu Windows, réactivez-le après l'installation et ouvrez individuellement les ports du serveur Windows IaaS. Reportez-vous à [Ports de serveur Windows IaaS](#).

- Placez tous les serveurs IaaS Windows sur le même domaine. N'utilisez pas de groupes de travail.
- Chaque serveur nécessite la configuration matérielle minimale suivante.
 - 2 CPU
 - 8 Go de mémoire
 - 40 Go de stockage sur disque

Un serveur qui héberge la base de données SQL en même temps que des composants IaaS peut nécessiter du matériel supplémentaire.

- Les serveurs Windows IaaS et l'hôte de la base de données SQL Server doivent pouvoir se résoudre mutuellement via leur nom NETBIOS. Si nécessaire, ajoutez les noms NETBIOS au fichier `/etc/hosts` sur chaque serveur Windows IaaS et sur l'hôte de la base de données SQL Server, puis redémarrez les machines.
- En raison de la demande de ressources matérielles, n'effectuez pas de déploiement sur VMware Workstation.
- Installez Microsoft .NET Framework 3.5.
- Installez Microsoft .NET Framework 4.5.2 ou version ultérieure.

Un exemplaire de .NET est disponible à partir de n'importe quel dispositif vRealize Automation :

`https://vrealize-automation-appliance-FQDN:5480/installer`

Si vous utilisez Internet Explorer pour le téléchargement, vérifiez que l'option de configuration de sécurité renforcée n'est pas activée. Accédez à `res://iesetup.dll/SoftAdmin.htm` sur le serveur Windows.

- Installez Microsoft PowerShell 3.0 ou 4.0, en fonction de votre version de Windows.

Certaines mises à niveau ou migrations de vRealize Automation peuvent nécessiter l'installation d'une version plus ancienne ou plus récente de PowerShell, en plus de celle que vous utilisez actuellement.

- Pour tout déploiement d'une taille supérieure à la valeur minimale, définissez Serveurs Windows IaaS sur les paramètres régionaux anglais.

- Si vous installez plusieurs composants IaaS sur le même serveur Windows, prévoyez de les installer dans le même dossier d'installation. N'utilisez pas des chemins d'accès distincts.
- Les serveurs IaaS utilisent TLS à des fins d'authentification, une option activée par défaut sur certains serveurs Windows.

Certains sites désactivent TLS pour des raisons de sécurité, mais vous devez laisser au moins un protocole TLS activé. Cette version de vRealize Automation prend en charge TLS 1.2.

- Activez le service DTC (Distributed Transaction Coordinator). IaaS utilise DTC pour les transactions de base de données et les actions telles que la création de workflows.

Note Si vous clonez une machine pour créer un serveur Windows IaaS, installez DTC sur le clone après le clonage. Si vous clonez une machine disposant déjà de DTC, son identifiant unique est copié sur le clone, ce qui entraîne l'échec de la communication. Reportez-vous à [Erreur dans la communication de Manager Service](#).

Activez également DTC sur le serveur qui héberge la base de données SQL, si elle est distincte de IaaS. Pour en savoir plus sur l'activation de DTC, consultez [Article 2038943 de la base de connaissances VMware](#).

- Vérifiez que le service de connexion secondaire est en cours d'exécution. Si vous le souhaitez, vous pouvez arrêter le service une fois l'installation terminée.

Ports de serveur Windows IaaS

Les ports sur les serveurs Windows IaaS doivent être configurés avant l'installation de vRealize Automation.

Ouvrez les ports entre tous les serveurs de Windows IaaS conformément aux tableaux suivants. Incluez le serveur qui héberge la base de données SQL, si ce n'est pas IaaS. Sinon, si les stratégies du site le permettent, vous pouvez désactiver les pare-feu situés entre les serveurs Windows IaaS et SQL Server.

Tableau 2-4. Ports entrants

Port	Protocole	Composant	Commentaires
443	TCP	Manager Service	Communication avec les composants IaaS et le dispositif vRealize Automation sur HTTPS.
443	TCP	Dispositif vRealize Automation	Communication avec les composants IaaS et le dispositif vRealize Automation sur HTTPS.
443	TCP	Hôtes des points de terminaison de l'infrastructure	Communication avec les composants IaaS et le dispositif vRealize Automation sur HTTPS. En général, le port 443 est le port de communication par défaut des hôtes des points de terminaison de l'infrastructure virtuelle et de cloud, mais reportez-vous à la documentation fournie par vos hôtes d'infrastructure pour obtenir la liste complète des ports par défaut et des ports requis

Tableau 2-4. Ports entrants (suite)

Port	Protocole	Composant	Commentaires
443	TCP	Agent invité agent de démarrage logiciel	Communication avec Manager Service sur HTTPS
443	TCP	DEM Worker	Communication avec NSX Manager
1433	TCP	Instance du serveur SQL Server	MSSQL

Tableau 2-5. Ports sortants

Port	Protocole	Composant	Commentaires
53	TCP, UDP	Tout	DNS
67, 68, 546, 547	TCP, UDP	Tout	DHCP
123	TCP, UDP	Tout	Facultatif. NTP
443	TCP	Manager Service	Communication avec le dispositif vRealize Automation sur HTTPS
443	TCP	Instances de Distributed Execution Manager	Communication avec Manager Service sur HTTPS
443	TCP	Agents proxy	Communication avec Manager Service et les hôtes des points de terminaison de l'infrastructure sur HTTPS
443	TCP	Agent de gestion	Communication avec le dispositif vRealize Automation
443	TCP	Agent invité agent de démarrage logiciel	Communication avec Manager Service sur HTTPS
1433	TCP	Manager Service Site Web	MSSQL
5480	TCP	Tout	Communication avec le dispositif vRealize Automation.

En outre, comme vous activez DTC entre tous les serveurs, DTC nécessite le port 135 sur TCP et un port aléatoire entre 1 024 et 65 535. Notez que le vérificateur de conditions préalables vérifie que DTC est en cours d'exécution et que les ports requis sont ouverts.

Serveur Web IaaS

Un serveur Windows qui héberge le composant Web doit répondre à des conditions requises supplémentaires, en plus de celles applicables à tous les serveurs Windows IaaS.

Les conditions requises sont les mêmes, que le composant Web héberge ou non Model Manager.

- Configurez Java.
 - Installez Java 64 bits 1.8, mise à jour 191. N'utilisez pas la version 32 bits.

JRE est suffisant. Vous n'avez pas besoin du JDK complet.

- Définissez la variable d'environnement JAVA_HOME sur le dossier d'installation de Java.
- Vérifiez que le fichier %JAVA_HOME%\bin\java.exe est disponible.
- Configurez IIS (Internet Information Services) en fonction du tableau suivant.

Vous avez besoin d'IIS 7.5 pour les variantes de Windows 2008, d'IIS 8 pour Windows 2012, d'IIS 8.5 pour Windows 2012 R2 et d'IIS 10 pour Windows 2016.

Outre les paramètres de configuration, évitez d'héberger des sites Web supplémentaires dans IIS. vRealize Automation définit la liaison sur son port de communication sur toutes les adresses IP non attribuées, ce qui ne permet aucune autre liaison. Le port de communication par défaut de vRealize Automation est le port 443.

Tableau 2-6. IaaS Internet Information Services

Composant IIS	Configuration
Rôles Internet Information Services (IIS)	<ul style="list-style-type: none"> ■ Authentification Windows ■ Contenu statique ■ Document par défaut ■ ASPNET 3.5 et ASPNET 4.5 ■ Extensions ISAPI ■ Filtre ISAPI
Service d'activation des processus IIS Windows	<ul style="list-style-type: none"> ■ API de configuration ■ Environnement NET ■ Modèle de processus ■ Activation de Windows Communication Foundation (variantes de Windows 2008 uniquement) ■ Activation HTTP ■ Activation non-HTTP (variantes de Windows 2008 uniquement) <p>(Variantes de Windows 2012 : accédez à Fonctions > Fonctionnalités de .Net Framework 3.5 > Activation Non-HTTP)</p>
Paramètres d'authentification IIS	<p>Définissez les valeurs autres que par défaut suivantes.</p> <ul style="list-style-type: none"> ■ Authentification Windows activée ■ Authentification anonyme désactivée <p>Ne modifiez pas les valeurs par défaut suivantes.</p> <ul style="list-style-type: none"> ■ Fournisseur Negotiate activé ■ Fournisseur NTLM activé ■ Authentification Windows en mode kernel activée ■ Protection étendue pour l'authentification Windows désactivée ■ Pour les certificats qui utilisent SHA512, TLS1.2 doit être désactivé sur les variantes de Windows 2012

Hôte Manager Service IaaS

Un serveur Windows qui héberge le composant Manager Service doit respecter des conditions requises supplémentaires, en plus de celles de tous les serveurs Windows IaaS.

Il ne peut exister aucun pare-feu entre un hôte Manager Service et l'hôte DEM. Pour plus d'informations, reportez-vous à la section [Ports de serveur Windows IaaS](#).

Les conditions requises sont identiques si l'hôte Manager Service est une instance principale ou secondaire.

Hôte du serveur SQL IaaS

Un serveur Windows qui héberge la base de données SQL IaaS doit satisfaire certaines conditions requises.

Votre serveur SQL peut résider sur l'un des serveurs Windows IaaS ou sur un hôte distinct. Lors d'un hébergement avec des composants IaaS, les conditions requises s'ajoutent à celles applicables à tous les serveurs Windows IaaS.

- Cette version de vRealize Automation ne prend pas en charge le mode de compatibilité 130 de SQL Server 2016 par défaut. Si vous créez séparément une base de données SQL Server 2016 vide pour l'utiliser avec IaaS, utilisez le mode de compatibilité 100 ou 120.

Si vous créez la base de données à l'aide du programme d'installation vRealize Automation, la compatibilité est déjà configurée.

Le même comportement s'applique également à SQL Server 2017.

- La fonctionnalité Groupe de disponibilité AlwaysOn (AAG) est uniquement prise en charge avec SQL Server 2016 Entreprise ou SQL Server 2017 Entreprise. Lorsque vous utilisez AAG, spécifiez le nom de domaine complet de l'écouteur AAG en tant qu'hôte SQL Server. Lors de la création de l'AAG, définissez DTC_Support = Per_DB. La définition du paramètre après la création de l'AAG ne fonctionnera pas.
- Lors d'un hébergement avec IaaS, configurez Java.
 - Installez Java 64 bits 1.8, Update 181 ou version ultérieure. N'utilisez pas la version 32 bits. JRE est suffisant. Vous n'avez pas besoin du JDK complet.
 - Définissez la variable d'environnement JAVA_HOME sur le dossier d'installation de Java.
 - Vérifiez que le fichier %JAVA_HOME%\bin\java.exe est disponible.
- Utilisez une version prise en charge de SQL Server indiquée dans la [Matrice de support de vRealize Automation](#).
- Activez le protocole TCP/IP pour SQL Server.
- SQL Server inclut un modèle de base de données applicable à toutes les bases de données créées sur l'instance de SQL. Pour qu'IaaS s'installe correctement, ne modifiez pas la taille du modèle de base de données.

- Généralement, le serveur nécessite plus de matériel que les indications minimales fournies dans [Serveurs Windows IaaS](#).

Pour plus d'informations, reportez-vous aux *Spécifications matérielles et capacités maximales* du guide de *Architecture de référence* vRealize Automation.

- Avant d'exécuter le programme d'installation de vRealize Automation, vous devez identifier les comptes et ajouter des autorisations dans SQL. Reportez-vous à [Comptes et mots de passe](#).

Hôte DEM (Distributed Execution Manager) IaaS

Un serveur Windows qui héberge le composant DEM (Distributed Execution Manager)

Orchestrator ou Worker doit répondre aux conditions requises supplémentaires, en plus de celles de tous les serveurs Windows IaaS.

Il ne peut exister aucun pare-feu entre un hôte DEM et l'hôte Manager Service. Pour plus d'informations, reportez-vous à la section [Ports de serveur Windows IaaS](#).

Les DEM Workers peuvent avoir des conditions requises supplémentaires selon les ressources de provisionnement avec lesquelles ils interagissent.

DEM Workers avec Amazon Web Services

Un DEM Worker vRealize AutomationIaaS qui communique avec Amazon Web Services (AWS) doit respecter des conditions requises supplémentaires, en plus de celles de tous les serveurs de Windows IaaS et de DEM en général.

Un DEM Worker peuvent communiquer avec AWS pour le provisionnement. Le DEM Worker communique avec un compte Amazon EC2 et collecte des données sur ce compte.

- Le DEM Worker doit avoir accès à Internet.
- Si le DEM Worker se trouve derrière un pare-feu, le trafic HTTPS doit être autorisé vers et depuis `aws.amazon.com` ainsi que vers et depuis les URL des régions EC2 auxquelles vos comptes AWS ont accès, par exemple `ec2.us-east-1.amazonaws.com` pour la région Est des États-Unis.

Chaque URL assure la résolution de plusieurs adresses IP, c'est pourquoi vous devrez peut-être utiliser un outil, comme celui disponible sur le site Internet des solutions réseau, pour répertorier et configurer ces adresses IP.

- Si le DEM Worker a accès à Internet par un serveur proxy, le service DEM doit s'exécuter sous des informations d'identification pouvant être authentifiées sur le serveur proxy.

DEM Workers avec Openstack ou PowerVC

Un DEM Worker vRealize AutomationIaaS qui communique avec Openstack ou PowerVC et collecte des données de ces derniers doit satisfaire des conditions requises supplémentaires, en plus de celles de tous les serveurs Windows IaaS et des DEM en général.

Tableau 2-7. Configuration requise des DEM Workers Openstack et PowerVC

Votre installation	Configuration requise
Tout	<p>Dans la base de Registre Windows, activez la prise en charge de TLS v1.2 pour .NET Framework. Par exemple :</p> <pre>[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319] "SchUseStrongCrypto"=dword:00000001</pre> <pre>[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319] "SchUseStrongCrypto"=dword:00000001</pre>
Hôte DEM Windows 2008	<p>Dans la base de Registre Windows, activez le protocole TLS v1.2. Par exemple :</p> <pre>[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2] [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client] "DisabledByDefault"=dword:00000000 "Enabled"=dword:00000001</pre> <pre>[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server] "DisabledByDefault"=dword:00000000 "Enabled"=dword:00000001</pre>
Certificats auto-signés sur votre hôte de point de terminaison d'infrastructure	<p>Si votre instance de PowerVC ou d'Openstack n'utilise pas de certificats approuvés, importez le certificat SSL à partir de votre instance de PowerVC ou d'Openstack dans le magasin d'autorités de certification racine approuvées sur chaque serveur IaaS Windows sur lequel vous souhaitez installer un DEM vRealize Automation.</p>

DEM Workers avec virtualisation Red Hat

Un DEM Worker vRealize Automation IaaS qui communique avec RHEV (Red Hat Enterprise Virtualization) et collecte des données de ce dernier doit satisfaire des conditions supplémentaires, en plus de celles de tous les serveurs Windows IaaS et des DEM en général.

- Vous devez joindre chaque environnement RHEV au domaine contenant le serveur DEM Worker.
- Les informations d'identification utilisées pour gérer le point de terminaison représentant un environnement RHEV doivent disposer des privilèges d'administrateur sur l'environnement RHEV. Lorsque vous utilisez RHEV pour le provisionnement, le DEM Worker communique avec ce compte et collecte des données de celui-ci.
- Ces informations d'identification doivent également disposer de suffisamment de privilèges pour créer des objets sur les hôtes dans l'environnement.

DEM Workers avec SCVMM

Un DEM Worker vRealize AutomationaaS qui gère les machines virtuelles via SCVMM (System Center Virtual Machine Manager) doit satisfaire des conditions supplémentaires, en plus de celles de tous les serveurs Windows IaaS et des DEM en général.

- Installez le DEM Worker sur la même machine avec la console SCVMM.

Il est recommandé d'installer la console SCVMM sur une machine DEM Worker distincte.

- Le DEM Worker doit avoir accès au module SCVMM PowerShell installé avec la console.
- La stratégie d'exécution de PowerShell doit être définie sur RemoteSigned ou Unrestricted.

Pour vérifier la stratégie d'exécution de PowerShell, exécutez l'une des commandes suivantes à l'invite de commandes PowerShell.

```
help about_signing
help Set-ExecutionPolicy
```

- Si tous les DEM Workers dans l'instance ne se trouvent pas sur des machines répondant à ces conditions requises, utilisez des commandes Skill pour diriger les workflows associés à SCVMM vers des DEM Workers qui s'y trouvent.

vRealize Automation ne prend pas en charge un environnement de déploiement qui utilise une configuration de cloud privé SCVMM. vRealize Automation ne peut actuellement pas collecter de données à partir de clouds privés SCVMM, et y effectuer des affectations ou des provisionnements.

Les conditions requises supplémentaires suivantes s'appliquent à SCVMM.

- vRealize Automation prend en charge SCVMM 2012 R2, qui nécessite PowerShell 3 ou version ultérieure.
- Vous devez installer la console SCVMM avant d'installer des DEM Workers vRealize Automation qui consomment des éléments de travail SCVMM.

Si vous installez DEM Worker avant la console SCVMM, des journaux d'erreurs semblables à l'exemple suivant s'affichent :

Le workflow « ScvmmEndpointDataCollection » a échoué avec l'exception suivante : le terme « Get-VMMServer » n'est pas reconnu comme le nom d'un applet de commande, d'une fonction, d'un fichier de script ou d'un programme fonctionnel. Vérifiez l'orthographe du nom ou, si un chemin d'accès était inclus, assurez-vous que le celui-ci est correct et réessayez.

Pour résoudre ce problème, vérifiez que la console SCVMM est installée et redémarrez le service DEM Worker.

- Chaque instance de SCVMM doit être associée au domaine contenant le serveur.
- Les informations d'identification utilisées pour gérer le point de terminaison représentant une instance SCVMM doivent disposer des privilèges d'administrateur sur le serveur SCVMM.

Les informations d'identification doivent également donner droit aux privilèges d'administrateur sur les serveurs Hyper-V au sein de l'instance.

- Pour provisionner des machines sur une ressource SCVMM, l'utilisateur vRealize Automation qui demande l'article du catalogue doit avoir le rôle d'administrateur dans l'instance de SCVMM.
- Les serveurs Hyper-V situés dans une instance de SCVMM é gérer doivent être des serveurs Windows 2008 R2 SP1 sur lesquels Hyper-V est installé. Le processeur doit être équipé des extensions de virtualisation requises .NET Framework 4.5.2 ou version ultérieure doit être installé et Windows Management Instrumentation (WMI) doit être activé.
- Pour provisionner une machine Generation-2 sur une ressource SCVMM 2012 R2, vous devez ajouter les propriétés suivantes au Blueprint.

```
Scvmm.Generation2 = true
Hyperv.Network.Type = synthetic
```

Les Blueprints Generation-2 doivent avoir un vHDX (virtualHardDisk) de données collectées existant dans la page d'information du build du Blueprint. S'il est vide, le provisionnement Generation-2 échoue.

Pour plus d'informations sur la préparation de votre environnement SCVMM, reportez-vous à *Configuration de vRealize Automation*.

Certificats

vRealize Automation utilise des certificats SSL pour la communication sécurisée entre les composants IaaS et les instances du dispositif vRealize Automation. Les dispositifs et les machines d'installation Windows échangent ces certificats afin d'établir une connexion fiable. Vous pouvez obtenir des certificats auprès d'une autorité de certification interne ou externe, ou générer des certificats auto-signés lors du processus de déploiement de chaque composant.

Pour obtenir d'importantes informations sur le dépannage, la prise en charge et les conditions d'approbation des certificats, consultez [Article 2106583 de la base de connaissances VMware](#).

Note vRealize Automation prend en charge les certificats SHA2. Les certificats auto-signés générés par le système utilisent SHA-256 avec le chiffrement RSA. Vous devrez éventuellement procéder à une mise à jour vers les certificats SHA2 en raison de conditions requises du système d'exploitation ou du navigateur.

Vous pouvez mettre à jour ou remplacer des certificats après le déploiement. Par exemple, un certificat peut expirer ou vous pouvez choisir d'utiliser des certificats auto-signés lors de votre déploiement initial, mais vous devez ensuite obtenir des certificats auprès d'une autorité de confiance avant la mise en service de vRealize Automation.

Tableau 2-8. Mise en œuvre des certificats

Composant	Déploiement minimal (hors production)	Déploiement distribué (prêt pour production)
Dispositif vRealize Automation	Générez un certificat auto-signé lors de la configuration du dispositif.	Pour chaque cluster de dispositifs, vous pouvez utiliser un formulaire de certificat d'une autorité de certification interne ou externe. Les certificats à usage multiple et les génériques sont pris en charge.
Les composants de IaaS	Lors de l'installation, acceptez les certificats auto-signés générés ou sélectionnez la suppression des certificats.	Obtenez un certificat à usage multiple, tel qu'un certificat Subject Alternative Name (SAN), auprès d'une autorité de certification interne ou externe que votre client Web approuve.

Chaînes de certificats

Si vous utilisez des chaînes de certificats, spécifiez les certificats dans l'ordre suivant :

- Certificat client/serveur signé par le certificat CA intermédiaire
- Un ou plusieurs certificats intermédiaires
- Un certificat CA racine

Incluez l'en-tête BEGIN CERTIFICATE et le pied de page END CERTIFICATE pour chaque certificat lorsque vous importez des certificats.

Modifications d'un certificat en cas de personnalisation de l'URL de connexion de vRealize Automation

Si vous souhaitez que les utilisateurs se connectent à un nom d'URL autre que celui d'un dispositif ou d'un équilibrage de charge vRealize Automation, consultez les étapes CNAME précédant ou suivant l'installation dans [Définissez l'URL de connexion à vRealize Automation sur un nom personnalisé](#).

Exigences en matière de certificats vRealize Automation

Lors de l'utilisation de vos propres certificats avec vRealize Automation, les certificats doivent répondre à certaines exigences.

Types de certificats pris en charge

Dans de nombreuses organisations, les certificats sont émis ou requis par des autorités externes en fonction des exigences de l'entreprise.

Les exigences suivantes concernent le format d'identité courant et les types de certificats utilisés avec des déploiements vRealize Automation classiques.

Propriété de certificat	Configuration requise
Algorithme de hachage	SHA1, SHA2, (256, 584, 512)
Algorithme de signature	RSASSA-PKCS1_V1_5
Longueur de clé	2048, 4096

Note La signature RSASSA-PSS n'est pas prise en charge pour les déploiements vRealize Automation. Cette signature est la valeur par défaut pour une autorité de certification Microsoft sous Windows 2012 R2. La signature étant un paramètre configurable, vous devez vous assurer qu'elle est correctement configurée lorsque vous utilisez une autorité de certification Microsoft.

Matrice de prise en charge de certificats vRealize Automation

Algorithme de hachage	SHA1				SHA2-256			
	RSASSA-PKCS1_V1_5		RSASSA-PSS		RSASSA-PKCS1_V1_5		RSASSA-PSS	
Algorithme de signature								
Taille de la clé	2048	4096	2048	4096	2048	4096	2048	4096
vRealize Automation pris en charge	Prise en charge vérifié	Prise en charge vérifié	Non pris en charge	Non pris en charge	Prise en charge vérifié	Prise en charge vérifié	Non pris en charge	Non pris en charge

Algorithme de hachage	SHA2-384				SHA2-512			
	RSASSA-PKCS1_V1_5		RSASSA-PSS		RSASSA-PKCS1_V1_5		RSASSA-PSS	
Algorithme de signature								
Taille de la clé	2048	4096	2048	4096	2048	4096	2048	4096
vRealize Automation pris en charge	Prise en charge vérifié	Prise en charge vérifié	Non pris en charge	Non pris en charge	Prise en charge vérifié	Prise en charge vérifié	Non pris en charge	Non pris en charge

Extraction de certificats et de clés privées

Les certificats des dispositifs virtuels doivent être au format PEM.

Si votre autorité de certification a fourni un certificat au format PFX, utilisez OpenSSL pour convertir PFX en PEM.

```
openssl pkcs12 -in path-to-pfx -out desired-path-to-pem -nodes
```

Par exemple :

```
openssl pkcs12 -in C:\vra-cert.pfx -out C:\vra-cert.pem -nodes
```

vous pouvez être invité à entrer une phrase secrète si le certificat PFX en incluait une.

Déploiement du dispositif vRealize Automation

3

Le dispositif vRealize Automation est livré en tant que fichier de virtualisation ouvert que vous pouvez déployer sur une infrastructure virtualisée existante.

Ce chapitre contient les rubriques suivantes :

- [À propos du déploiement du dispositif vRealize Automation](#)
- [Déployer le dispositif vRealize Automation](#)
- [Ajouter des contrôleurs d'interface réseau avant d'exécuter le programme d'installation](#)

À propos du déploiement du dispositif vRealize Automation

Toutes les installations nécessitent d'abord un dispositif vRealize Automation déployé mais non configuré, avant que vous n'utilisiez l'une des options d'installation vRealize Automation réelles.

- Assistant d'installation consolidé basé sur navigateur
- Configuration de dispositif basée sur navigateur distincte, suivie par des installations Windows distinctes pour les serveurs IaaS
- Programme d'installation silencieux basé sur une ligne de commande qui accepte une entrée provenant d'un fichier de propriétés de réponses
- API REST d'installation qui accepte une entrée au format JSON

Déployer le dispositif vRealize Automation

Avant de pouvoir prendre l'un des chemins d'installation, vRealize Automation vous impose de déployer au moins un dispositif vRealize Automation .

Pour créer le dispositif, vous utilisez le client vSphere pour télécharger et déployer une machine virtuelle partiellement configurée à partir d'un modèle. Vous devrez éventuellement exécuter la procédure plusieurs fois, si vous prévoyez de créer un déploiement d'entreprise pour la haute disponibilité et le basculement. Ce type de déploiement dispose généralement de plusieurs dispositifs vRealize Automation derrière un équilibrage de charge.

Conditions préalables

- Connectez-vous au client vSphere avec un compte qui a l'autorisation de déployer des modèles OVF dans l'inventaire.
- Téléchargez le fichier .ovf ou .ova du dispositif vRealize Automation à un emplacement accessible par le client vSphere.

Procédure

- 1 Sélectionnez l'option vSphere **Déployer le modèle OVF**.
- 2 Entrez le chemin d'accès au fichier .ovf ou .ova du dispositif vRealize Automation.
- 3 Examinez les détails du modèle.
- 4 Lisez et acceptez le contrat de licence d'utilisateur final.
- 5 Entrez un nom de dispositif et un emplacement d'inventaire.

Lorsque vous déployez des dispositifs, utilisez un nom différent pour chacun d'eux et n'incluez pas dans les noms des caractères non alphanumériques tels que des traits de soulignement (_).

- 6 Sélectionnez l'hôte et le cluster dans lesquels le dispositif va résider.
- 7 Sélectionnez le pool de ressources dans lequel le dispositif va résider.
- 8 Sélectionnez le stockage qui hébergera le dispositif.
- 9 Sélectionnez un format de disque.

Les formats statiques améliorent les performances et les formats dynamiques économisent de l'espace de stockage.

Le format n'a pas d'incidence sur la taille de disque du dispositif. Si un dispositif nécessite plus d'espace pour les données, ajoutez des disques à l'aide de vSphere après le déploiement.

- 10 Dans le menu déroulant, sélectionnez un réseau de Destination.
- 11 Terminez les propriétés du dispositif.

- a Entrez et confirmez un mot de passe racine.

Les informations d'identification du compte racine vous connectent à l'interface Web d'administration hébergée par le dispositif ou à la console de ligne de commande du système d'exploitation du dispositif.

- b Indiquez s'il convient ou non d'autoriser les connexions SSH à distance à la console de ligne de commande.

La désactivation de SSH est plus sécurisée, mais vous devez accéder directement à la console dans vSphere plutôt que via un client Terminal Server distinct.

- c Pour le **Nom d'hôte**, entrez le nom de domaine complet du dispositif.

Pour de meilleurs résultats, entrez le nom de domaine complet, même si vous utilisez DHCP.

Note vRealize Automation prend en charge DHCP, mais des adresses IP statiques sont recommandées pour les déploiements de production.

- d Dans les propriétés du réseau, lorsque vous utilisez des adresses IP statiques, entrez les valeurs de passerelle, de masque de réseau et de serveurs DNS. Vous devez également entrer l'adresse IP, le nom de domaine complet et le domaine pour le dispositif, comme indiqué dans l'exemple suivant.

Figure 3-1. Exemple de propriétés de dispositif virtuel

▼ Application	3 settings
Enable SSH service in the appliance	This will be used as an initial status of the SSH service in the appliance. You can change it later from the appliance Web console. <input checked="" type="checkbox"/>
Hostname	The host name for this virtual machine. Provide the fully qualified domain name if you use a static IP. Leave blank to try to reverse look up the IP address if you use DHCP. <input type="text" value="va1.mycompany.com"/>
Initial root password	This will be used as an initial password for the root user account. You can change the password later (by using the passwd command or from the appliance Web console). Enter password <input type="password" value="*****"/> Confirm password <input type="password" value="*****"/>
▼ Networking Properties	6 settings
Default Gateway	The default gateway address for this VM. Leave blank if DHCP is desired. <input type="text" value="12.34.56.79"/>
Domain Name	The domain name of this VM. Leave blank if DHCP is desired. <input type="text" value="mycompany.com"/>
Domain Name Servers	The domain name server IP Addresses for this VM (comma separated). Leave blank if DHCP is desired. <input type="text" value="12.34.56.80, 12.34.56.81"/>
Domain Search Path	The domain search path (comma or space separated domain names) for this VM. Leave blank if DHCP is desired. <input type="text" value="mycompany.com"/>
Network 1 IP Address	The IP address for this interface. Leave blank if DHCP is desired. <input type="text" value="12.34.56.78"/>
Network 1 Netmask	The netmask or prefix for this interface. Leave blank if DHCP is desired. <input type="text" value="255.255.254.0"/>

- 12 Selon votre déploiement, vCenter Server et la configuration de DNS, sélectionnez l'une des manières suivantes de terminer le déploiement et la mise sous tension du dispositif.

- Si vous avez procédé au déploiement sur vSphere et si **Mettre sous tension après le déploiement** est disponible sur la page Prêt à terminer, procédez comme suit.
 - a Sélectionnez l'option **Mettre sous tension après le déploiement**, puis cliquez sur **Terminer**.

- b Une fois que le fichier a terminé le déploiement dans vCenter Server, cliquez sur **Fermer**.
 - c Attendez le démarrage de la machine virtuelle, qui peut prendre jusqu'à 5 minutes.
 - Si vous avez procédé au déploiement sur vSphere et si **Mettre sous tension après le déploiement** n'est pas disponible sur la page Prêt à terminer, procédez comme suit.
 - a Une fois que le fichier a terminé le déploiement dans vCenter Server, cliquez sur **Fermer**.
 - b Mettez sous tension le dispositif vRealize Automation.
 - c Attendez le démarrage de la machine virtuelle, qui peut prendre jusqu'à 5 minutes.
 - d Vérifiez que le dispositif vRealize Automation est déployé en envoyant une interrogation ping à son nom de domaine complet. Si vous ne pouvez pas envoyer une interrogation ping au dispositif, redémarrez la machine virtuelle.
 - e Attendez le démarrage de la machine virtuelle, qui peut prendre jusqu'à 5 minutes.
 - Si vous avez déployé le dispositif vRealize Automation sur vCloud en utilisant vCloud Director, vCloud peut remplacer le mot de passe que vous avez entré lors du déploiement OVA. Pour empêcher le remplacement, procédez comme suit.
 - a Après le déploiement dans vCloud Director, cliquez sur vApp pour voir le dispositif vRealize Automation.
 - b Cliquez avec le bouton droit sur le dispositif vRealize Automation, puis sélectionnez **Propriétés**.
 - c Cliquez dans l'onglet **Personnalisation du système d'exploitation invité**.
 - d Sous **Réinitialisation du mot de passe**, désactivez l'option **Autoriser le mot de passe d'administrateur local**, puis cliquez sur **OK**.
 - e Mettez sous tension le dispositif vRealize Automation.
 - f Attendez le démarrage de la machine virtuelle, qui peut prendre jusqu'à 5 minutes.
- 13** Vérifiez que le dispositif vRealize Automation est déployé en envoyant une interrogation ping à son nom de domaine complet.

Étape suivante

- (Facultatif) Ajoutez des cartes réseau. Reportez-vous à [Ajouter des contrôleurs d'Interface réseau avant d'exécuter le programme d'installation](#).
- Connectez-vous à l'interface Web d'administration pour exécuter l'assistant d'installation consolidée ou pour configurer manuellement le dispositif.
 https://vrealize-automation-appliance-FQDN:5480
- Sinon, vous pouvez ignorer la connexion afin de tirer parti de l'installation de vRealize Automation silencieuse ou basée sur API.

Ajouter des contrôleurs d'Interface réseau avant d'exécuter le programme d'installation

vRealize Automation prend en charge plusieurs contrôleurs d'interface réseau (NIC). Avant d'exécuter le programme d'installation, il est possible d'ajouter des cartes réseau au dispositif vRealize Automation ou au serveur Windows IaaS.

Si plusieurs cartes réseau doivent être en place avant l'exécution de l'assistant d'installation vRealize Automation, ajoutez-les après le déploiement dans vCenter, mais avant de démarrer l'assistant. Exemples de raisons pouvant justifier la mise en place précoce de cartes réseau :

- Vous souhaitez séparer les réseaux utilisateur et infrastructure.
- Vous avez besoin d'une carte réseau supplémentaire afin que les serveurs IaaS puissent joindre un domaine Active Directory.

Pour plus d'informations sur les multiples scénarios de carte réseau, consultez cette [publication du blog VMware Cloud Management](#).

En présence de trois cartes réseau ou plus, tenez compte des limitations suivantes.

- VIDM a besoin d'accéder à la base de données Postgres et à Active Directory.
- Dans un cluster HA, VIDM a besoin d'accéder à l'URL d'équilibrage de charge.
- Les connexions de VIDM précédentes doivent provenir des deux premières cartes réseau.
- Les cartes réseau venant après la deuxième carte réseau ne doivent pas être utilisées ni reconnues par VIDM.
- Les cartes réseau venant après la deuxième carte réseau ne doivent pas être utilisées pour se connecter à Active Directory.

Utilisez la première ou la seconde carte réseau lors de la configuration d'un annuaire dans vRealize Automation.

Conditions préalables

Déployez le fichier OVF du dispositif vRealize Automation et les machines virtuelles Windows, mais n'ouvrez pas de session ou ne démarrez pas l'assistant d'installation.

Procédure

- 1 Dans vCenter, ajoutez des cartes réseau à chaque dispositif vRealize Automation.
 - a Cliquez avec le bouton droit sur le dispositif récemment déployé et sélectionnez **Modifier les paramètres**.
 - b Ajoutez des cartes réseau VMXNETn.
 - c S'il est sous tension, redémarrez le dispositif.
- 2 Connectez-vous à la ligne de commande du dispositif vRealize Automation en tant qu'utilisateur racine.

- 3 Configurez les cartes réseau en exécutant la commande suivante pour chaque carte réseau.

Assurez-vous d'inclure l'adresse de passerelle par défaut. Vous pouvez configurer des itinéraires statiques après avoir terminé cette procédure.

```
/opt/vmware/share/vami/vami_set_network network-interface (STATICV4|STATICV4+DHCPV6|
STATICV4+AUTOV6) IPv4-addressnetmaskgateway-v4-address
```

Par exemple :

```
/opt/vmware/share/vami/vami_set_network eth1 STATICV4 192.168.100.20 255.255.255.0
192.168.100.1
```

- 4 Vérifiez que tous les nœuds vRealize Automation peuvent se résoudre mutuellement par nom DNS.
- 5 Vérifiez que tous les nœuds vRealize Automation peuvent accéder à des noms de domaine complets à équilibrage de charge pour les composants vRealize Automation.
- 6 Si vous utilisez Split-Brain DNS, vérifiez que tous les nœuds vRealize Automation et les adresses IP virtuelles ont le même nom de domaine complet dans DNS pour l'adresse IP et l'adresse IP virtuelle (VIP) de chaque nœud.
- 7 Dans vCenter, ajoutez des cartes réseau aux serveurs Windows IaaS.
 - a Cliquez avec le bouton droit sur le serveur IaaS et sélectionnez **Modifier les paramètres**.
 - b Ajoutez des cartes réseau à la machine virtuelle du serveur IaaS.
- 8 Sous Windows, configurez les cartes réseau du serveur IaaS ajoutées et leurs adresses IP. Si nécessaire, consultez la documentation Microsoft.

Étape suivante

- (Facultatif) Si vous avez besoin d'itinéraires statiques, suivez les directives dans [Configurer des routes statiques](#) avant de poursuivre l'installation.
- Connectez-vous à l'interface Web d'administration pour exécuter l'assistant d'installation consolidée ou pour configurer manuellement le dispositif.
<https://vrealize-automation-appliance-FQDN:5480>
- Sinon, vous pouvez ignorer la connexion afin de tirer parti de l'installation de vRealize Automation silencieuse ou basée sur API.

Installation de vRealize Automation avec l'assistant Installation

4

L'assistant d'installation de vRealize Automation permet d'installer simplement et rapidement des déploiements minimaux ou d'entreprise.

Avant de lancer l'assistant, vous devez déployer un dispositif vRealize Automation et configurer les serveurs Windows IaaS conformément aux conditions préalables. L'assistant d'installation s'affiche lors de votre première connexion au dispositif vRealize Automation qui vient d'être déployé.

- Pour arrêter l'assistant afin d'y revenir plus tard, cliquez sur **Fermer la session**.
- Pour désactiver l'assistant, cliquez sur **Annuler** ou déconnectez-vous et commencez l'installation manuelle par le biais des interfaces standard.

L'assistant est l'outil de base pour les nouvelles installations de vRealize Automation. Si vous souhaitez développer un déploiement de vRealize Automation existant après avoir exécuté l'assistant, reportez-vous aux procédures décrites dans la section [Chapitre 5 Les interfaces d'installation standard de vRealize Automation](#).

Ce chapitre contient les rubriques suivantes :

- [Utilisation de l'assistant d'installation pour des déploiements minimaux](#)
- [Utilisation de l'assistant d'installation pour les déploiements d'entreprise](#)

Utilisation de l'assistant d'installation pour des déploiements minimaux

Les déploiements minimaux démontrent le fonctionnement de vRealize Automation mais n'ont généralement pas suffisamment de capacité pour prendre en charge les environnements de production d'entreprise.

Installez un déploiement minimal pour un travail de validation technique ou pour vous familiariser avec vRealize Automation.

Démarrer l'assistant d'installation pour un déploiement minimal

Les déploiements minimaux consistent, en général, en un dispositif vRealize Automation, un serveur Windows IaaS et l'agent vSphere pour les points de terminaison. Une installation minimale place tous les composants IaaS sur un serveur Windows unique.

Conditions préalables

- Traitez les conditions préalables de [Chapitre 2 Préparation à l'installation de vRealize Automation](#).
- Créer un dispositif non configuré. Reportez-vous à [Déployer le dispositif vRealize Automation](#).

Procédure

- 1 Connectez-vous à l'interface d'administration du dispositif vRealize Automation en tant qu'utilisateur racine.

`https://vrealize-automation-appliance-FQDN:5480`
- 2 Lorsque l'assistant d'installation s'affiche, cliquez sur **Suivant**.
- 3 Acceptez le contrat de licence, puis cliquez sur **Suivant**.
- 4 Sur la page Type de déploiement, sélectionnez **Déploiement minimal** et **Installer les infrastructures en tant que service**, puis cliquez sur **Suivant**.
- 5 Sur la page Conditions préalables d'installation, connectez-vous au serveur IaaS Windows et installez l'agent de gestion. L'agent de gestion permet au dispositif vRealize Automation de détecter ces serveurs IaaS et de s'y connecter.

Étape suivante

Installez l'agent de gestion sur vos serveurs Windows IaaS. Reportez-vous à [Installer l'agent de gestion vRealize Automation](#).

Installer l'agent de gestion vRealize Automation

Tous les serveurs Windows IaaS ont besoin de l'agent de gestion, lequel les lie à leur dispositif vRealize Automation spécifique.

Si vous hébergez la base de données SQL Server vRealize Automation sur une machine Windows distincte qui n'héberge pas de composants IaaS, la machine SQL Server n'a pas besoin de l'agent de gestion.

L'agent de gestion enregistre le serveur Windows IaaS dans le dispositif vRealize Automation spécifique, automatise l'installation et la gestion des composants IaaS et collecte les informations de télémétrie et d'assistance. L'agent de gestion s'exécute comme un service Windows dans un compte de domaine avec des droits d'administrateur sur les serveurs Windows IaaS.

Conditions préalables

Créez un dispositif vRealize Automation et lancez l'assistant d'installation.

Reportez-vous à la section [Déployer le dispositif vRealize Automation](#) et [Démarrer l'assistant d'installation pour un déploiement minimal](#).

Procédure

- 1 Connectez-vous à la console du dispositif vRealize Automation en tant qu'utilisateur racine.
- 2 Entrez la commande suivante :

```
openssl x509 -in /opt/vmware/etc/lighttpd/server.pem -fingerprint -noout -sha1
```
- 3 Copiez l'empreinte digitale afin de pouvoir la vérifier plus tard. Par exemple :

```
71:84:47:72:03:57:C8:C2:68:65:00:06:BC:D8:23:98:92:54:BF:89
```
- 4 Connectez-vous au serveur Windows IaaS en utilisant un compte disposant des droits d'administrateur.
- 5 Ouvrez un navigateur Web à l'URL du programme d'installation de vRealize Automation.

```
https://vrealize-automation-appliance-FQDN:5480/installer
```
- 6 Cliquez sur **Programme d'installation de l'agent de gestion**, puis enregistrez et exécutez le fichier .msi.
- 7 Lisez le message d'accueil.
- 8 Acceptez l'accord de licence d'utilisateur final.
- 9 Acceptez ou modifiez le dossier d'installation.

```
Program Files (x86)\VMware\VCAC\Management Agent
```


10 Entrez les détails du dispositif vRealize Automation :

- a Entrez l'adresse HTTPS du dispositif, y compris le nom de domaine complet et le numéro de port :5480.
- b Entrez les informations d'identification du compte racine du dispositif.
- c Cliquez sur **Charger** et assurez-vous que l'empreinte digitale correspond à celle précédemment copiée. Ignorez les deux-points.

Si les empreintes digitales ne correspondent pas, assurez-vous que vous disposez de l'adresse correcte du dispositif.

Figure 4-1. Agent de gestion - Détails du dispositif vRealize Automation

11 Entrez le domaine\nom d'utilisateur et le mot de passe du compte de service.

Le compte de service doit être un compte de domaine disposant des droits d'administrateur sur les serveurs Windows IaaS. Utilisez partout le même compte de service.

12 Suivez les invites pour terminer l'installation de l'agent de gestion.**Résultats**

Note Comme ils sont liés, vous devez réinstaller l'agent de gestion si vous remplacez le dispositif vRealize Automation.

La désinstallation de composants IaaS d'un serveur Windows ne supprime pas l'agent de gestion. Pour désinstaller un agent de gestion, utilisez séparément l'option Ajouter ou supprimer des programmes de Windows.

Étape suivante

Revenez à l'assistant d'installation basé sur navigateur. Les serveurs Windows IaaS pour lesquels l'agent de gestion est installé apparaissent sous Hôtes découverts.

Exécution de l'assistant d'installation

Après l'installation de l'agent de gestion, revenez à l'assistant et suivez les invites. Si vous avez besoin d'obtenir des instructions supplémentaires sur les paramètres, cliquez sur le lien d'aide dans le coin supérieur droit de l'assistant.

- Lorsque vous avez terminé l'assistant, la dernière page affiche le chemin d'accès et le nom d'un fichier de propriétés. Vous pouvez modifier le fichier et l'utiliser pour effectuer une installation silencieuse de vRealize Automation avec des paramètres identiques ou similaires à ceux de votre session de l'assistant. Reportez-vous à [Chapitre 6 Installation silencieuse de vRealize Automation](#).
- Si vous avez créé le contenu initial, vous pouvez vous connecter au locataire par défaut en tant qu'utilisateur configurationadmin et demander les éléments du catalogue.
- Pour configurer l'accès au locataire par défaut pour d'autres utilisateurs, reportez-vous à la section [Configurer l'accès au locataire par défaut](#).

Utilisation de l'assistant d'installation pour les déploiements d'entreprise

Vous pouvez adapter votre déploiement d'entreprise aux besoins de votre organisation. Un déploiement d'entreprise peut se composer de composants distribués ou de déploiements de haute disponibilité configurés avec des équilibres de charge.

Les déploiements d'Entreprise sont conçus pour des structures d'installation plus complexes avec des composants distribués et redondants et incluent généralement des équilibres de charge. L'installation des composants IaaS est facultative, quel que soit le type de déploiement.

Pour les déploiements équilibrés en charge, la présence de plusieurs instances de serveur Web actives et dispositifs vRealize Automation font échouer l'installation. Une seule instance de serveur Web et un seul dispositif vRealize Automation doivent être actifs pendant l'installation.

Démarrer l'assistant d'installation pour un déploiement d'entreprise

Les déploiements d'entreprise sont assez volumineux pour les environnements de production. Vous pouvez utiliser l'assistant d'installation pour déployer une installation distribuée ou une installation distribuée avec équilibres de charge pour la haute disponibilité et le basculement.

Si vous déployez une installation distribuée avec équilibres de charge, informez le responsable d'équipe de configurer votre environnement vRealize Automation. Vos administrateurs de locataires doivent configurer la fonctionnalité de gestion des annuaires pour la haute disponibilité lorsqu'ils configurent le lien vers Active Directory.

Conditions préalables

- Traitez les conditions préalables de [Chapitre 2 Préparation à l'installation de vRealize Automation](#).
- Créer un dispositif non configuré. Reportez-vous à [Déployer le dispositif vRealize Automation](#).

Procédure

- 1 Connectez-vous à l'interface d'administration du dispositif vRealize Automation en tant qu'utilisateur racine.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Lorsque l'assistant d'installation s'affiche, cliquez sur **Suivant**.
- 3 Acceptez le contrat de licence d'utilisateur final, puis cliquez sur **Suivant**.
- 4 Sur la page Type de déploiement, sélectionnez **Déploiement d'entreprise** et **Installer les infrastructures en tant que service**.
- 5 Sur la page Conditions préalables d'installation, connectez-vous aux serveurs IaaS Windows et installez l'agent de gestion. L'agent de gestion permet au dispositif vRealize Automation de détecter ces serveurs IaaS et de s'y connecter.

Étape suivante

Installez l'agent de gestion sur vos serveurs Windows IaaS. Reportez-vous à [Installer l'agent de gestion vRealize Automation](#).

Installer l'agent de gestion vRealize Automation

Tous les serveurs Windows IaaS ont besoin de l'agent de gestion, lequel les lie à leur dispositif vRealize Automation principal.

Si vous hébergez la base de données SQL Server vRealize Automation sur une machine Windows distincte qui n'héberge pas de composants IaaS, la machine SQL Server n'a pas besoin de l'agent de gestion.

L'agent de gestion enregistre le serveur Windows IaaS dans le dispositif vRealize Automation principal, automatise l'installation et la gestion des composants IaaS, et collecte les informations de télémétrie et de support. L'agent de gestion s'exécute comme un service Windows dans un compte de domaine avec des droits d'administrateur sur les serveurs Windows IaaS.

Conditions préalables

Créez un ou plusieurs dispositifs vRealize Automation et lancez l'assistant d'installation.

Reportez-vous à la section [Déployer le dispositif vRealize Automation](#) et [Démarrer l'assistant d'installation pour un déploiement d'entreprise](#).

Procédure

- 1 Connectez-vous à la console du dispositif vRealize Automation principal en tant qu'utilisateur racine.
- 2 Entrez la commande suivante :
`openssl x509 -in /opt/vmware/etc/lighttpd/server.pem -fingerprint -noout -sha1`

- 3 Copiez l'empreinte digitale afin de pouvoir la vérifier plus tard. Par exemple :

71:84:47:72:03:57:C8:C2:68:65:00:06:BC:D8:23:98:92:54:BF:89

- 4 Connectez-vous au serveur Windows IaaS en utilisant un compte disposant des droits d'administrateur.

- 5 Ouvrez un navigateur Web à l'URL du programme d'installation du dispositif vRealize Automation principal.

<https://vrealize-automation-appliance-FQDN:5480/installer>

- 6 Cliquez sur **Programme d'installation de l'agent de gestion**, puis enregistrez et exécutez le fichier .msi.

- 7 Lisez le message d'accueil.

- 8 Acceptez l'accord de licence d'utilisateur final.

- 9 Acceptez ou modifiez le dossier d'installation.

Program Files (x86)\VMware\VCAC\Management Agent

- 10 Entrez les détails du dispositif vRealize Automation principal :

- a Entrez l'adresse HTTPS du dispositif principal, y compris le nom de domaine complet et le numéro de port 5480.
- b Entrez les informations d'identification du compte racine du dispositif principal.
- c Cliquez sur **Charger** et assurez-vous que l'empreinte digitale correspond à celle précédemment copiée. Ignorez les deux-points.

Si les empreintes digitales ne correspondent pas, assurez-vous que vous disposez de l'adresse correcte du dispositif.

Figure 4-2. Agent de gestion - Détails du dispositif vRealize Automation

- 11 Entrez le domaine\nom d'utilisateur et le mot de passe du compte de service.

Le compte de service doit être un compte de domaine disposant des droits d'administrateur sur les serveurs Windows IaaS. Utilisez partout le même compte de service.

- 12 Suivez les invites pour terminer l'installation de l'agent de gestion.

Résultats

Répétez la procédure pour tous les serveurs Windows qui hébergeront des composants IaaS.

Note Comme ils sont liés, vous devez réinstaller l'agent de gestion si vous remplacez le dispositif vRealize Automation.

La désinstallation de composants IaaS d'un serveur Windows ne supprime pas l'agent de gestion. Pour désinstaller un agent de gestion, utilisez séparément l'option Ajouter ou supprimer des programmes de Windows.

Étape suivante

Revenez à l'assistant d'installation basé sur navigateur. Les serveurs Windows IaaS pour lesquels l'agent de gestion est installé apparaissent sous Hôtes découverts.

Exécution de l'assistant d'installation

Après l'installation de l'agent de gestion, revenez à l'assistant et suivez les invites. Si vous avez besoin d'obtenir des instructions supplémentaires sur les paramètres, cliquez sur le lien d'aide dans le coin supérieur droit de l'assistant.

- Lorsque vous avez terminé l'assistant, la dernière page affiche le chemin d'accès et le nom d'un fichier de propriétés. Vous pouvez modifier le fichier et l'utiliser pour effectuer une installation silencieuse de vRealize Automation avec des paramètres identiques ou similaires à ceux de votre session de l'assistant. Reportez-vous à [Chapitre 6 Installation silencieuse de vRealize Automation](#).
- Si vous avez créé le contenu initial, vous pouvez vous connecter au locataire par défaut en tant qu'utilisateur configurationadmin et demander les éléments du catalogue.
- Pour configurer l'accès au locataire par défaut pour d'autres utilisateurs, reportez-vous à la section [Configurer l'accès au locataire par défaut](#).

Les interfaces d'installation standard de vRealize Automation

5

Après l'exécution de l'assistant d'installation, vous devrez ou souhaiterez éventuellement effectuer certaines tâches d'installation manuellement au moyen des interfaces standard.

L'assistant d'installation décrit dans [Chapitre 4 Installation de vRealize Automation avec l'assistant Installation](#) constitue votre principal outil pour procéder à de nouvelles installations de vRealize Automation. Cependant, après l'exécution de l'assistant, certaines opérations nécessitent toujours l'ancien processus d'installation manuelle.

Vous devez exécuter les étapes manuelles si vous souhaitez étendre un déploiement vRealize Automation ou si l'assistant s'est arrêté pour une raison quelconque. Voici des exemples de situations dans lesquelles vous devrez éventuellement vous reporter aux procédures suivantes.

- Vous choisissez d'annuler l'assistant avant de terminer l'installation.
- Échec de l'installation au moyen de l'assistant.
- Vous souhaitez ajouter un autre dispositif vRealize Automation pour la haute disponibilité.
- Vous souhaitez ajouter un autre serveur Web IaaS pour la haute disponibilité.
- Vous avez besoin d'un autre agent proxy.
- Vous avez besoin d'un autre DEM Worker ou Orchestrator.

Vous pouvez utiliser l'ensemble ou seulement une partie des processus manuels. Consultez les informations fournies dans cette section et suivez les procédures qui s'appliquent à votre situation.

Ce chapitre contient les rubriques suivantes :

- [Utilisation des interfaces standard pour des déploiements minimaux](#)
- [Utilisation des interfaces standard pour les déploiements distribués](#)
- [Installation d'agents vRealize Automation](#)

Utilisation des interfaces standard pour des déploiements minimaux

Vous pouvez installer un déploiement minimal autonome à utiliser dans un environnement de développement ou en tant que validation technique. Les déploiements minimaux ne sont pas adaptés à un environnement de production.

Liste de contrôle pour un déploiement minimal

Installez vRealize Automation dans une configuration minimale de validation technique ou de travaux de développement. Les déploiements minimaux nécessitent moins d'étapes, mais ne disposent pas de la capacité de production d'un déploiement d'entreprise.

Effectuez les tâches de haut niveau dans l'ordre suivant.

Tableau 5-1. Liste de contrôle pour un déploiement minimal

Tâche	Détails
<input type="checkbox"/> Prévoyez les conditions préalables de l'installation de l'environnement et de l'adresse.	Chapitre 2 Préparation à l'installation de vRealize Automation
<input type="checkbox"/> Créez un dispositif vRealize Automation non configuré.	Déployer le dispositif vRealize Automation
<input type="checkbox"/> Configurez manuellement le dispositif vRealize Automation.	Configurer le dispositif vRealize Automation
<input type="checkbox"/> Installez les composants IaaS sur un seul serveur Windows.	Installation des composants IaaS
<input type="checkbox"/> Installez des agents supplémentaires, au besoin.	Installation d'agents vRealize Automation
<input type="checkbox"/> Effectuez des tâches de post-installation comme la configuration du locataire par défaut.	Configurer l'accès au locataire par défaut

Configurer le dispositif vRealize Automation

Le dispositif vRealize Automation est une machine virtuelle partiellement configurée qui héberge le serveur vRealize Automation et le portail Web d'utilisateur. Vous téléchargez et déployez le modèle OVF (Open Virtualization Format) vers vCenter Server ou l'inventaire ESX/ESXi.

Conditions préalables

- Créer un dispositif non configuré. Reportez-vous à [Déployer le dispositif vRealize Automation](#).
- Obtenez un certificat d'authentification pour le dispositif vRealize Automation.

Procédure

- 1 Connectez-vous à la nouvelle interface de gestion de dispositif vRealize Automation en tant qu'utilisateur racine.

`https://vrealize-automation-appliance-FQDN:5480`

Continuez après l'affichage éventuel des avertissements de certificat.

- Si l'assistant d'installation s'affiche, annulez-le afin de pouvoir accéder à l'interface de gestion plutôt qu'à l'assistant.
- Sélectionnez **Admin > Paramètres de l'heure** et définissez la source de synchronisation de l'heure.

Option	Description
Heure de l'hôte	Se synchroniser avec l'hôte ESXi du dispositif vRealize Automation.
Serveur de temps	Se synchroniser avec un serveur NTP (Network Time Protocol) externe. Entrez le nom de domaine complet ou l'adresse IP du serveur NTP.

Vous devez synchroniser les dispositifs vRealize Automation et les serveurs IaaS Windows avec la même source de temps. Ne mélangez pas les sources de temps au sein d'un déploiement vRealize Automation.

- Sélectionnez **vRA > Paramètres de l'hôte**.

Option	Action
Résoudre automatiquement	Sélectionnez Résoudre automatiquement pour spécifier le nom de l'hôte actuel du dispositif vRealize Automation.
Mise à jour de l'hôte	<p>Pour les nouveaux hôtes, sélectionnez Mise à jour de l'hôte. Entrez le nom de domaine complet du dispositif vRealize Automation, <i>vra-hostname.domain.name</i>, dans la zone de texte Nom d'hôte.</p> <p>Pour les déploiements distribués qui utilisent des équilibres de charge, sélectionnez Mise à jour de l'hôte. Entrez le nom de domaine complet du serveur d'équilibrage de charge, <i>vra-loadbalancename.domain.name</i>, dans la zone de texte Nom d'hôte.</p>

Note Configurez les paramètres SSO de la manière décrite plus loin dans cette procédure lorsque vous utilisez **Mise à jour de l'hôte** pour définir le nom d'hôte.

- Sélectionnez l'action appropriée dans le menu **Action de certificat**.

Si vous utilisez un certificat codé au format PEM, pour un environnement distribué par exemple, sélectionnez **Importer**.

Les certificats que vous importez doivent être approuvés et être également applicables à toutes les instances de dispositif vRealize Automation et à tous les équilibres de charge par le biais de l'utilisation de certificats SAN (autre nom de l'objet).

Si vous souhaitez générer une demande CSR pour un nouveau certificat que vous pouvez envoyer à une autorité de certification, sélectionnez **Générer une demande de signature**. Une CSR permet à votre autorité de certification de créer un certificat avec les valeurs correctes que vous pouvez importer.

Note Si vous utilisez des chaînes de certificats, spécifiez les certificats dans l'ordre suivant :

- a Certificat client/serveur signé par le certificat CA intermédiaire
- b Un ou plusieurs certificats intermédiaires
- c Un certificat CA racine

Option	Action
Conserver l'existant	Conserver la configuration SSL actuelle. Sélectionnez cette option pour annuler vos modifications.
Générer un certificat	<ul style="list-style-type: none">a La valeur affichée dans la zone de texte Nom commun est celle du nom d'hôte, tel qu'il s'affiche dans la partie supérieure de la page. Si des instances supplémentaires du dispositif vRealize Automation sont disponibles, leurs noms de domaine complets sont inclus dans l'attribut SAN du certificat.b Entrez le nom de votre organisation, comme le nom de votre société, dans la zone de texte Organisation.c Entrez votre unité d'organisation, comme le nom ou l'emplacement de votre service, dans la zone de texte Unité d'organisation.d Entrez un code pays ISO 3166, comme FR, dans la zone de texte Pays.

Option	Action
Générer une demande de signature	<ul style="list-style-type: none"> a Sélectionnez Générer une demande de signature. b Passez en revue les entrées dans les zones de texte Organisation, Unité d'organisation, Code du pays et Nom commun. Ces entrées sont remplies à partir du certificat existant. Vous pouvez modifier ces entrées si nécessaire. c Cliquez sur Générer une CSR pour générer un demande de signature de certificat, puis cliquez sur le lien Télécharger la demande CSR générée ici pour ouvrir une boîte de dialogue qui vous permet d'enregistrer la CSR à un emplacement d'où vous pouvez l'envoyer à une autorité de certification. d Lorsque vous recevez le certificat préparé, cliquez sur Importer et suivez les instructions permettant d'importer un certificat dans vRealize Automation.
Importer	<ul style="list-style-type: none"> a Copiez les valeurs du certificat de BEGIN PRIVATE KEY à END PRIVATE KEY, en incluant l'en-tête et le pied de page, et collez-les dans la zone de texte Clé privée RSA. b Copiez les valeurs du certificat de BEGIN CERTIFICATE à END CERTIFICATE, en incluant l'en-tête et le pied de page, dans la zone de texte Chaîne de certificat. Pour les valeurs de certificats multiples, incluez un en-tête BEGIN CERTIFICATE et un pied de page END CERTIFICATE pour chaque certificat. <hr/> <p>Note Dans le cas de certificats en chaînes, des attributs supplémentaires peuvent être disponibles.</p> <ul style="list-style-type: none"> c (Facultatif) Si votre certificat utilise une phrase secrète pour chiffrer la clé de certificat, copiez la phrase secrète et collez-la dans la zone de texte Phrase secrète.

- 6 Cliquez sur **Enregistrer les paramètres** pour enregistrer les informations de l'hôte et la configuration SSL.
- 7 Configurez les paramètres SSO.
- 8 Cliquez sur **Messagerie**. Les paramètres de configuration et l'état de la messagerie pour votre dispositif s'affichent. Ne modifiez pas ces paramètres.
- 9 Cliquez sur l'onglet **Télémétrie** pour indiquer si vous souhaitez participer au programme d'amélioration du produit de VMware (CEIP).

Pour en savoir plus sur les données collectées au titre du CEIP et leur utilisation par VMware, consultez le Trust & Assurance Center à l'adresse <http://www.vmware.com/trustvmware/ceip.html>.

- Cochez la case **Rejoindre le programme d'amélioration du produit de VMware** pour participer au programme.
- Désactivez la case **Rejoindre le programme d'amélioration du produit de VMware** pour ne pas participer au programme.

- 10** Cliquez sur **Services** et vérifiez que des services sont enregistrés.

Selon la configuration de votre site, cela peut prendre environ 10 minutes.

Note Vous pouvez vous connecter au dispositif et exécuter `tail -f /var/log/vcac/catalina.out` pour surveiller le démarrage des services.

- 11** Saisissez les informations sur votre licence.

- a Cliquez sur **vRA > Attribution de licence**.
- b Cliquez sur **Attribution de licence**.
- c Entrez une clé de licence vRealize Automation valide que vous avez téléchargée lors du téléchargement des fichiers d'installation, puis cliquez sur **Envoyer la clé**.

Note Si vous obtenez une erreur de connexion, l'équilibrage de charge peut présenter un problème. Vérifiez la connectivité réseau à l'équilibrage de charge.

- 12** Vérifiez que vous pouvez vous connecter à vRealize Automation.

- a Ouvrez un navigateur Web et accédez à l'URL de l'interface produit de vRealize Automation.

`https://vrealize-automation-appliance-FQDN/vcac`
- b Acceptez le certificat vRealize Automation.
- c Acceptez le certificat SSO.
- d Connectez-vous avec l'identifiant `administrator@vsphere.local` et le mot de passe que vous avez spécifié lorsque vous avez configuré SSO.

L'interface s'ouvre sur la page Locataires dans l'onglet **Administration**. Un locataire nommé `vsphere.local` figure dans la liste.

Résultats

Vous avez terminé le déploiement et la configuration de votre dispositif vRealize Automation. Si le dispositif ne fonctionne pas correctement après la configuration, redéployez et reconfigurez le dispositif. N'apportez pas de modifications au dispositif existant.

Étape suivante

Reportez-vous à [Installer les composants d'infrastructure](#).

Installation des composants IaaS

L'administrateur installe un ensemble complet de composants d'infrastructure (IaaS) sur une machine Windows (physique ou virtuelle). Des droits d'administrateur sont requis pour effectuer ces tâches.

Une installation minimale installe tous les composants sur le même serveur Windows, excepté pour la base de données SQL, que vous pouvez installer sur un serveur distinct.

Activer la synchronisation de l'heure sur le serveur Windows

Les horloges sur le serveur vRealize Automation et les serveurs Windows doivent être synchronisées pour que l'installation réussisse.

La procédure suivante décrit comment activer la synchronisation de l'heure avec l'hôte ESX/ESXi en utilisant VMware Tools. Si vous installez les composants IaaS sur un hôte physique ou si vous ne souhaitez pas utiliser VMware Tools pour la synchronisation de l'heure, assurez-vous que l'heure du serveur est exacte en utilisant la méthode que vous préférez.

Procédure

- 1 Ouvrez une invite de commande sur la machine d'installation Windows.
- 2 Entrez la commande suivante pour accéder au répertoire VMware Tools.

```
cd C:\Program Files\VMware\VMware Tools
```

- 3 Tapez la commande pour afficher l'état de synchronisation de l'heure.

```
VMwareToolboxCmd.exe timesync status
```

- 4 Si la synchronisation de l'heure est désactivée, entrez la commande suivante pour l'activer.

```
VMwareToolboxCmd.exe timesync enable
```

Certificats IaaS

Les composants IaaS de vRealize Automation utilisent des certificats et SSL pour sécuriser les communications entre les composants. Dans une installation minimale à des fins de preuve de concept, vous pouvez utiliser des certificats auto-signés.

Dans un environnement distribué, obtenez un certificat de domaine auprès d'une autorité de certification de confiance. Pour obtenir des informations sur l'installation de certificats de domaine pour les composants IaaS, reportez-vous à [Installer des certificats IaaS](#) dans le chapitre consacré au déploiement distribué.

Installer les composants d'infrastructure

L'administrateur système se connecte à la machine Windows et utilise l'assistant d'installation pour installer les services IaaS sur la machine virtuelle ou physique Windows.

Conditions préalables

- Vérifiez que le serveur répond aux exigences dans la section [Serveurs Windows IaaS](#).
- [Activer la synchronisation de l'heure sur le serveur Windows](#).

- Vérifiez que vous avez déployé et configuré entièrement le dispositif vRealize Automation, et que les services nécessaires sont en cours d'exécution (plugin-service, catalog-service, iaas-proxy-provider).

Procédure

1 Télécharger le programme d'installation de vRealize AutomationIaaS

Pour installer IaaS sur votre serveur Windows minimal virtuel ou physique, vous téléchargez une copie du programme d'installation d'IaaS à partir du dispositif vRealize Automation.

2 Sélectionner le type d'installation

L'administrateur système exécute l'assistant du programme d'installation sur la machine d'installation Windows 2008 ou 2012.

3 Vérifier les conditions préalables

L'outil de vérification des conditions préalables vérifie que votre machine répond aux conditions requises pour l'installation d'IaaS.

4 Spécifier les paramètres de serveur et de compte

L'administrateur système vRealize Automation spécifie les paramètres de serveur et de compte du serveur d'installation Windows et sélectionne une instance de serveur de base de données SQL et une méthode d'authentification.

5 Spécifier les gestionnaires et les agents

L'installation minimale installe les DEM requis et l'agent proxy vSphere par défaut. L'administrateur système peut installer des agents proxy supplémentaires (XenServer ou Hyper-V, par exemple) après l'installation à l'aide du programme d'installation personnalisé.

6 Enregistrer les composants IaaS

L'administrateur système installe le certificat IaaS et enregistre les composants IaaS avec le SSO.

7 Terminer l'installation

L'administrateur système termine l'installation d'IaaS.

Télécharger le programme d'installation de vRealize AutomationIaaS

Pour installer IaaS sur votre serveur Windows minimal virtuel ou physique, vous téléchargez une copie du programme d'installation d'IaaS à partir du dispositif vRealize Automation.

Si des avertissements de certificat s'affichent pendant ce processus, continuez après ces avertissements pour terminer l'installation.

Conditions préalables

- Passez en revue la configuration requise du serveur Windows IaaS. Reportez-vous à [Serveurs Windows IaaS](#).

- Si vous utilisez Internet Explorer pour le téléchargement, vérifiez que l'option de configuration de sécurité renforcée n'est pas activée. Accédez à `res://iesetup.dll/SoftAdmin.htm` sur le serveur Windows.

Procédure

- 1 Connectez-vous au serveur IaaS Windows en utilisant un compte ayant des droits d'administrateur.
- 2 Ouvrez un navigateur Web directement à l'URL du programme d'installation du dispositif vRealize Automation.

`https://vrealize-automation-appliance-FQDN:5480/installer`
- 3 Cliquez sur **Programme d'installation d'IaaS**.
- 4 Enregistrez `setup__vrealize-automation-appliance-FQDN@5480` sur le serveur Windows.

Ne modifiez pas le nom de fichier du programme d'installation. Il est utilisé pour connecter l'installation au dispositif vRealize Automation

Sélectionner le type d'installation

L'administrateur système exécute l'assistant du programme d'installation sur la machine d'installation Windows 2008 ou 2012.

Conditions préalables

[Télécharger le programme d'installation de vRealize AutomationIaaS](#).

Procédure

- 1 Cliquez avec le bouton droit sur le fichier d'installation `setup__vrealize-automation-appliance-FQDN@5480.exe` et sélectionnez **Exécuter en tant qu'administrateur**.
- 2 Cliquez sur **Suivant**.
- 3 Acceptez le contrat de licence, puis cliquez sur **Suivant**.
- 4 Sur la page de connexion, fournissez les informations d'identification d'administrateur pour le dispositif vRealize Automation et vérifiez le certificat SSL.
 - a Entrez le nom d'utilisateur **root** et le mot de passe.

Le mot de passe est celui que vous avez spécifié lors du déploiement du dispositif vRealize Automation.
 - b Sélectionnez **Accepter le certificat**.
 - c Cliquez sur **Afficher le certificat**.

Comparez l'empreinte de certificat à l'empreinte définie pour le dispositif vRealize Automation. Vous pouvez afficher le certificat du dispositif vRealize Automation dans le navigateur du client si vous avez accédé à l'interface de gestion du dispositif vRealize Automation sur le port 5480.

- 5 Sélectionnez **Accepter le certificat**.
- 6 Cliquez sur **Suivant**.
- 7 Sélectionnez **Installation complète** sur la page **Type d'installation** si vous créez un déploiement minimal et cliquez sur **Suivant**.

Vérifier les conditions préalables

L'outil de vérification des conditions préalables vérifie que votre machine répond aux conditions requises pour l'installation d'IaaS.

Conditions préalables

[Sélectionner le type d'installation.](#)

Procédure

- 1 Terminez la vérification des conditions préalables.

Option	Description
Aucune erreur	Cliquez sur Suivant .
Erreurs non critiques	Cliquez sur Aucune correction .
Erreurs critiques	Si vous ne corrigez pas les erreurs critiques, l'installation échoue. Si des avertissements s'affichent, sélectionnez l'avertissement dans le volet gauche et suivez les instructions à droite. Résolvez toutes les erreurs critiques et cliquez sur Vérifier à nouveau pour vérifier.

- 2 Cliquez sur **Suivant**.

Résultats

La machine répond aux conditions préalables pour l'installation.

Spécifier les paramètres de serveur et de compte

L'administrateur système vRealize Automation spécifie les paramètres de serveur et de compte du serveur d'installation Windows et sélectionne une instance de serveur de base de données SQL et une méthode d'authentification.

Conditions préalables

[Vérifier les conditions préalables.](#)

Procédure

- 1 Sur la page **Paramètres de serveur et de compte** ou sur la page **Paramètres détectés**, entrez le nom d'utilisateur et le mot de passe du compte de service Windows. Ce compte de service doit être un compte d'administrateur local disposant également de privilèges d'administration SQL.

2 Tapez une phrase dans la zone de texte **Phrase de passe**.

La phrase secrète est une série de mots qui génère la clé de chiffrement utilisée pour sécuriser les données de la base de données.

Note Enregistrez votre phrase secrète afin qu'elle soit disponible pour de futures installations ou une restauration du système.

3 Pour installer l'instance de base de données sur le même serveur que les composants IaaS, acceptez le serveur par défaut dans la zone de texte **Serveur** de la section Informations sur l'installation d'une base de données SQL Server.

Si la base de données se trouve sur une autre machine, indiquez le serveur au format suivant :

nom de domaine complet de la machine,numéro de port\instance de base de données nommée

4 Acceptez la valeur par défaut dans la zone de texte **Nom de la base de données** ou entrez le nom correspondant, au besoin.

5 Sélectionnez la méthode d'authentification.

- ◆ Sélectionnez **Utiliser l'authentification Windows** si vous souhaitez créer la base de données à l'aide des informations d'identification Windows de l'utilisateur actuel. L'utilisateur doit disposer de privilèges SQL sys_admin.
- ◆ Désélectionnez **Utiliser l'authentification Windows** si vous souhaitez créer la base de données à l'aide de l'authentification SQL. Tapez le **Nom d'utilisateur** and le **Mot de passe** de l'utilisateur du serveur SQL disposant de privilèges SQL sys_admin sur l'instance du serveur SQL.

L'authentification Windows est recommandée. Lorsque vous choisissez l'authentification SQL, le mot de passe de la base de données non chiffré figure dans certains fichiers de configuration.

6 (Facultatif) Cochez la case **Utiliser SSL pour la connexion à la base de données**.

Par défaut, la case est activée. SSL fournit une connexion plus sécurisée entre le serveur IaaS et la base de données SQL. Néanmoins, vous devez d'abord configurer le protocole SSL sur le serveur SQL pour prendre en charge cette option. Pour obtenir plus d'informations sur la configuration de SSL sur SQL Server, consultez [Article 189067 de Microsoft Technet](#).

7 Cliquez sur **Suivant**.

Spécifier les gestionnaires et les agents

L'installation minimale installe les DEM requis et l'agent proxy vSphere par défaut.

L'administrateur système peut installer des agents proxy supplémentaires (XenServer ou Hyper-V, par exemple) après l'installation à l'aide du programme d'installation personnalisé.

Conditions préalables

[Spécifier les paramètres de serveur et de compte.](#)

Procédure

- 1 Sur la page **DEM (Distributed Execution Managers) et agent proxy vSphere**, acceptez les valeurs par défaut ou modifiez les noms au besoin.
- 2 Acceptez la valeur par défaut pour installer un agent vSphere afin d'activer le provisionnement avec vSphere ou désélectionnez-la au besoin.
 - a Sélectionnez **Installer et configurer l'agent vSphere**.
 - b Acceptez l'agent et le point de terminaison par défaut ou tapez un nom.

Prenez note de la valeur du nom de point de terminaison. Vous devez taper cette information correctement au moment de configurer le point de terminaison vSphere sur la console vRealize Automation, sinon la configuration peut échouer.
- 3 Cliquez sur **Suivant**.

Enregistrer les composants IaaS

L'administrateur système installe le certificat IaaS et enregistre les composants IaaS avec le SSO.

Conditions préalables

[Télécharger le programme d'installation de vRealize AutomationIaaS.](#)

Procédure

- 1 Acceptez la valeur **Serveur** par défaut, qui est renseignée avec le nom de domaine complet du serveur du dispositif vRealize Automation à partir duquel vous avez téléchargé le programme d'installation. Vérifiez qu'un nom de domaine complet est utilisé pour identifier le serveur et non une adresse IP.

Si vous disposez de plusieurs dispositifs virtuels et que vous utilisez un équilibrage de charge, entrez le chemin d'accès au dispositif virtuel de l'équilibrage de charge.
- 2 Cliquez sur **Charger** pour renseigner la valeur du **Locataire par défaut SSO** (vsphere.local).
- 3 Cliquez sur **Télécharger** pour récupérer le certificat à partir du dispositif vRealize Automation.

Vous pouvez cliquer sur **Afficher le certificat** pour afficher les détails du certificat.
- 4 Sélectionnez **Accepter le certificat** pour installer le certificat SSO.
- 5 Dans le panneau Administrateur SSO, tapez **administrateur** dans la zone de texte **Nom d'utilisateur** et le mot de passe que vous avez défini pour cet utilisateur lorsque vous avez configuré l'authentification SSO dans **Mot de passe** et **Confirmez le mot de passe**.
- 6 Cliquez sur le lien de test à droite du champ **Nom d'utilisateur** pour valider le mot de passe entré.
- 7 Acceptez la valeur par défaut entrée dans **Serveur IaaS**, qui contient le nom d'hôte de la machine Windows sur laquelle vous effectuez l'installation.
- 8 Cliquez sur le lien de test à droite du champ **Serveur IaaS** pour valider la connectivité.

9 Cliquez sur **Suivant**.

Si des erreurs s'affichent après avoir cliqué sur **Suivant**, corrigez-les avant de poursuivre.

Terminer l'installation

L'administrateur système termine l'installation d'laaS.

Conditions préalables

- [Enregistrer les composants laaS.](#)
- Vérifiez que la machine sur laquelle vous procédez à l'installation est connectée au réseau et qu'elle est capable de se connecter au dispositif vRealize Automation à partir duquel vous téléchargez le programme d'installation d'laaS.

Procédure

- 1 Passez en revue l'information sur la page **Prêt à installer** et cliquez sur **Installer**.
L'installation démarre. En fonction de votre configuration réseau, l'installation peut prendre entre cinq minutes et une heure.
- 2 Lorsque le message de réussite apparaît, maintenez la case **Me guider tout au long de la configuration initiale** cochée, puis cliquez sur **Suivant** et sur **Terminer**.
- 3 Fermez la zone de message **Configurer le système**.

Résultats

L'installation est maintenant terminée.

Étape suivante

[Vérifier les services laaS.](#)

Utilisation des interfaces standard pour les déploiements distribués

Les déploiements d'entreprise sont conçus pour une plus grande capacité de vRealize Automation en production et nécessitent que vous distribuez des composants sur plusieurs machines. Les déploiements d'entreprise peuvent également inclure des systèmes redondants derrière les équilibres de charge.

Liste de contrôle d'un déploiement distribué

Un administrateur système peut déployer vRealize Automation dans une configuration distribuée, qui fournit une protection de basculement et une haute disponibilité par le biais de la redondance.

La liste de contrôle d'un déploiement distribué fournit une présentation générale des étapes requises pour effectuer une installation distribuée.

Tableau 5-2. Liste de contrôle d'un déploiement distribué

Tâche	Détails
<input type="checkbox"/> Planifiez et préparez l'environnement d'installation et vérifiez que toutes les conditions préalables pour l'installation sont remplies.	Chapitre 2 Préparation à l'installation de vRealize Automation
<input type="checkbox"/> Planifiez et obtenez vos certificats SSL.	Exigences de confiance du certificat dans un déploiement distribué
<input type="checkbox"/> Déployez le serveur du dispositif vRealize Automation principal, et tous les dispositifs supplémentaires nécessaires pour la redondance et la haute disponibilité.	Déployer le dispositif vRealize Automation
<input type="checkbox"/> Configurez votre équilibrage de charge pour gérer le trafic des dispositifs vRealize Automation.	Configuration de votre équilibrage de charge
<input type="checkbox"/> Configurez le serveur du dispositif vRealize Automation principal, et tous les dispositifs supplémentaires que vous avez déployés pour la redondance et la haute disponibilité.	Configuration de dispositifs pour vRealize Automation
<input type="checkbox"/> Configurez votre équilibrage de charge pour gérer le trafic des composants IaaS vRealize Automation et installez les composants IaaS vRealize Automation.	Installer les composants IaaS dans une configuration distribuée
<input type="checkbox"/> Le cas échéant, installez les agents pour l'intégration à des systèmes externes.	Installation d'agents vRealize Automation
<input type="checkbox"/> Configurez le locataire par défaut et fournissez la licence IaaS.	Configurer l'accès au locataire par défaut

vRealize Orchestrator

Le dispositif vRealize Automation inclut une version intégrée de vRealize Orchestrator dont l'utilisation est à présent recommandée avec les nouvelles installations. Dans les anciens déploiements ainsi que dans certains cas particuliers, les utilisateurs peuvent cependant connecter vRealize Automation à une instance externe distincte de vRealize Orchestrator. Reportez-vous à <https://www.vmware.com/products/vrealize-orchestrator.html>.

Pour obtenir des informations sur la connexion de vRealize Automation et de vRealize Orchestrator, reportez-vous à *Utilisation du plug-in vRealize Orchestrator pour vRealize Automation*.

Gestion des annuaires

Si vous effectuez une installation distribuée avec équilibrages de charge pour la haute disponibilité et le basculement, informez le responsable d'équipe pour qu'il configure votre environnement vRealize Automation. Vos administrateurs de locataires doivent configurer la fonctionnalité Gestion des annuaires en vue de la haute disponibilité lorsqu'ils configurent le lien vers votre Active Directory.

Pour plus d'informations sur la configuration de la gestion des annuaires pour la haute disponibilité, reportez-vous au guide *Configuration de vRealize Automation*.

Désactivation des contrôles de santé de l'équilibrage de charge

Les contrôles de santé garantissent qu'un équilibrage de charge envoie du trafic uniquement aux nœuds qui fonctionnent. L'équilibrage de charge envoie un contrôle de santé à une fréquence spécifiée à chaque nœud. Les nœuds qui dépassent le seuil d'échec deviennent inéligibles pour tout nouveau trafic.

Pour la distribution et le basculement de charges de travail, vous pouvez placer plusieurs dispositifs vRealize Automation derrière un équilibrage de charge. En outre, vous pouvez placer plusieurs serveurs Web IaaS et plusieurs serveurs Manager Service IaaS derrière leurs équilibres de charge respectifs.

Lors de l'utilisation d'équilibres de charge, n'autorisez pas les équilibres de charge à envoyer des contrôles de santé à tout moment pendant l'installation. Les contrôles de santé peuvent interférer avec l'installation ou provoquer chez celle-ci un comportement imprévisible.

- Lors du déploiement d'un dispositif vRealize Automation ou de composants IaaS derrière des équilibres de charge existants, désactivez les contrôles de santé sur tous les équilibres de charge dans la configuration proposée avant d'installer des composants.
- Après l'installation et la configuration de toutes les instances de vRealize Automation, notamment tous les dispositifs vRealize Automation et composants IaaS, vous pouvez réactiver les contrôles de santé.

Exigences de confiance du certificat dans un déploiement distribué

vRealize Automation utilise des certificats pour gérer les relations d'approbation et fournir une communication sécurisée entre les composants dans les déploiements distribués.

Dans un déploiement distribué ou en cluster, l'organisation de certificat suit largement l'architecture vRealize Automation à trois niveaux.

- Dispositifs vRealize Automation
- Composants Web IaaS
- Composants Manager Service IaaS

Dans un déploiement distribué, chaque machine d'un niveau donné partage un certificat. Par exemple, chaque dispositif vRealize Automation partage un certificat commun et chaque hôte Manager Service en partage également un commun.

Lorsque les composants Web et Manager Service sont hébergés sur la même machine, un certificat suffit pour les deux niveaux.

Certificats générés par le système

À partir de la version 7.0, si vous ne fournissez pas vos propres certificats, l'assistant d'installation de vRealize Automation peut générer automatiquement des certificats autosignés et les placer dans les magasins d'approbation appropriés sur les composants distribués qui en ont besoin.

Si vous devez mettre à jour des certificats autosignés générés par le système avec des certificats fournis par l'utilisateur ou l'autorité de certification, reportez-vous à *Gestion de vRealize Automation*.

Fournir vos propres certificats

Lors de l'exécution du programme d'installation manuel standard, vous fournissez des certificats autosignés que vous générez ou des certificats d'autorité de certification.

Lorsque vous fournissez ou générez vos propres certificats à l'aide d'OpenSSL ou d'une autre méthode, vous pouvez utiliser des certificats génériques ou des certificats SAN (Subject Alternative Name).

Les certificats IaaS doivent être des certificats à usage multiple. Lorsque vous fournissez des certificats, vous devez vous procurer un certificat polyvalent qui inclut les composants IaaS dans le cluster, puis copier ce certificat dans le magasin d'approbations pour chaque composant.

Équilibrages de charge

Pour la haute disponibilité et le basculement, vous pouvez ajouter des équilibrages de charge devant les composants vRealize Automation distribués. VMware recommande une configuration de relais pour les équilibrages de charge vRealize Automation. Dans une configuration de relais, les équilibrages de charge transmettent les demandes aux composants sans déchiffrement. Les dispositifs vRealize Automation et les hôtes IaaS effectuent ensuite le déchiffrement nécessaire.

Si vous utilisez des équilibrages de charge, vous devez inclure le nom de domaine complet de l'équilibrage de charge dans l'adresse approuvée des certificats polyvalents du cluster.

Pour plus d'informations sur l'utilisation et la configuration des équilibrages de charge, reportez-vous à la section *Équilibrage de charge vRealize Automation*.

Conditions d'approbation des certificats

Le tableau suivant récapitule les conditions d'enregistrement des approbations pour les certificats importés.

Importer	Enregistrer
Cluster de dispositif vRealize Automation	Cluster de composants Web IaaS
Cluster de composants Web IaaS	<ul style="list-style-type: none"> ■ Cluster de dispositif vRealize Automation ■ Cluster de composants Manager Service ■ Composants DEM Orchestrator et DEM Worker
Cluster de composants Manager Service IaaS	<ul style="list-style-type: none"> ■ Composants DEM Orchestrator et DEM Worker ■ Agents et agents proxy

Approbation de certificat et programme d'installation standard

Chaque fois que vous exécutez ou réexécutez le programme d'installation manuel standard pour créer des composants IaaS, vous devez configurer l'approbation de certificat sur ces composants IaaS. Par exemple, vous pouvez utiliser le programme d'installation standard pour monter en charge un déploiement existant.

■ Hôtes IaaS Web et Manager Service

Importez les fichiers `web.pfx` et `ms.pfx` dans les emplacements suivants.

```
Host Computer/Certificates/Personal certificate store
Host Computer/Certificates/Trusted People certificate store
```

■ Hôtes IaaS DEM Orchestrator, DEM Worker et agent proxy

Importez les fichiers `web.pfx` et `ms.pfx` dans l'emplacement suivant.

```
Host Computer/Certificates/Trusted People certificate store
```

Dans le magasin de certificats Trusted People, vous n'avez pas besoin d'importer la clé privée avec le certificat. Le processus d'installation automatique installe uniquement le certificat dans le magasin de certificats Trusted People.

Configurer une approbation de certificat pour des hôtes de composants Web, Manager Service et DEM

Les clients qui utilisent une empreinte numérique avec des fichiers PFX pré-installés pour prendre en charge l'authentification d'utilisateurs doivent configurer une approbation d'empreinte numérique sur l'hôte Web, Manager Service et sur les machines hôtes DEM Orchestrator et Worker.

Les clients qui importent des fichiers PEM ou utilisent des certificats auto-signés peuvent ignorer cette procédure.

Conditions préalables

Fichiers valides `web.pfx` et `ms.pfx` disponibles pour l'authentification par empreinte numérique.

Procédure

- 1 Importez les fichiers `web.pfx` et `ms.pfx` dans les emplacements suivants sur les machines hôtes de composants Web et Manager Service :

- *Host Computer/Certificates/Personal certificate store*
- *Host Computer/Certificates/Trusted People certificate store*

- 2 Importez les fichiers `web.pfx` et `ms.pfx` dans les emplacements suivants sur les machines hôtes DEM Orchestrator et Worker :

Host Computer/Certificates/Trusted People certificate store

- 3 Ouvrez une fenêtre Microsoft Management Console sur chacune des machines hôtes concernées.

Note Les chemins d'accès et options présentes sur Microsoft Management Console peuvent varier selon la version de Windows et la configuration du système.

- a Sélectionnez **Ajouter/Supprimer un composant logiciel enfichable**.
- b Sélectionnez **Certificats**.
- c Sélectionnez **Ordinateur local**.
- d Ouvrez les fichiers de certificats que vous avez précédemment importés et copiez les empreintes numériques.

Étape suivante

Insérez l'empreinte numérique dans la page Certificat de l'assistant vRealize Automation pour les composants Manager Service, Web Component et DEM.

Feuilles d'activité d'installation

Des feuilles de travail enregistrent d'importantes informations auxquelles vous devrez faire référence pendant l'installation.

Les paramètres sont sensibles à la casse. Notez la présence d'espaces supplémentaires pour d'autres composants, si vous installez un déploiement distribué. Vous n'aurez pas nécessairement besoin de tous les espaces des feuilles de travail. En outre, une machine peut héberger plusieurs composants IaaS. Par exemple, le serveur Web principal et le composant DEM Orchestrator peuvent avoir le même nom de domaine complet.

Tableau 5-3. Dispositif vRealize Automation

Variable	Ma valeur	Exemple
Nom de domaine complet du dispositif vRealize Automation principal		automation.mycompany.com
Adresse IP du dispositif principal vRealize Automation Pour référence uniquement ; n'entrez pas d'adresses IP		123.234.1.105
Nom de domaine complet du dispositif vRealize Automation supplémentaire		automation2.mycompany.com
Adresse IP du dispositif vRealize Automation supplémentaire Pour référence uniquement ; n'entrez pas d'adresses IP		123.234.1.106
Nom de domaine complet de l'équilibrage de charge du dispositif vRealize Automation		automation-balance.mycompany.com

Tableau 5-3. Dispositif vRealize Automation (suite)

Variable	Ma valeur	Exemple
Adresse IP de l'équilibrage de charge du dispositif vRealize Automation Pour référence uniquement ; n'entrez pas d'adresses IP		123.234.1.201
Nom d'utilisateur de l'interface de gestion (https://appliance-FQDN:5480)	racine (par défaut)	root
Mot de passe de l'interface de gestion		admin123
Locataire par défaut	vsphere.local (par défaut)	vsphere.local
Nom d'utilisateur du locataire par défaut	administrator@vsphere.local (par défaut)	administrator@vsphere.local
Mot de passe par défaut du locataire		login123

Tableau 5-4. Serveurs Windows IaaS

Variable	Ma valeur	Exemple
Serveur Web IaaS principal avec nom de domaine complet de Model Manager Data		web.mycompany.com
Serveur Web IaaS principal avec adresse IP de Model Manager Data Pour référence uniquement ; n'entrez pas d'adresses IP		123.234.1.107
Nom de domaine complet du serveur Web IaaS supplémentaire		web2.mycompany.com
Adresse IP du serveur Web IaaS supplémentaire Pour référence uniquement ; n'entrez pas d'adresses IP		123.234.1.108
Nom de domaine complet de l'équilibrage de charge du serveur Web IaaS		web-balance.mycompany.com
Adresse IP de l'équilibrage de charge du serveur Web IaaS Pour référence uniquement ; n'entrez pas d'adresses IP		123.234.1.202
Nom de domaine complet de l'hôte IaaS Manager Service actif		mgr-svc.mycompany.com
Adresses IP de l'hôte IaaS Manager Service actif Pour référence uniquement ; n'entrez pas d'adresses IP		123.234.1.109

Tableau 5-4. Serveurs Windows IaaS (suite)

Variable	Ma valeur	Exemple
Nom de domaine complet de l'hôte IaaS Manager Service passif		mgr-svc2.mycompany.com
Adresses IP de l'hôte IaaS Manager Service passif Pour référence uniquement ; n'entrez pas d'adresses IP		123.234.1.110
Nom de domaine complet de l'équilibrage de charge de l'hôte IaaS Manager Service		mgr-svc-balance.mycompany.com
Adresses IP de l'équilibrage de charge de l'hôte IaaS Manager Service Pour référence uniquement ; n'entrez pas d'adresses IP		123.234.203
Pour les services IaaS, compte de domaine avec droits d'administrateur sur les hôtes		SUPPORT\provisioner
Mot de passe du compte		login123

Tableau 5-5. Base de données IaaS SQL Server

Variable	Ma valeur	Exemple
Instance de base de données		IAASSQL
Nom de la base de données	vcac (par défaut)	vcac
Phrase secrète (utilisée lors de l'installation, de la mise à niveau et de la migration)		login123

Tableau 5-6. Instances d'IaaS Distributed Execution Manager

Variable	Ma valeur	Exemple
Nom de domaine complet de l'hôte DEM		dem.mycompany.com
Adresses IP de l'hôte DEM Pour référence uniquement ; n'entrez pas d'adresses IP		123.234.1.111
Nom de domaine complet de l'hôte DEM		dem2.mycompany.com
Adresses IP de l'hôte DEM Pour référence uniquement ; n'entrez pas d'adresses IP		123.234.1.112
Nom unique du composant DEM Orchestrator		Orchestrator-1

Tableau 5-6. Instances d'IaaS Distributed Execution Manager (suite)

Variable	Ma valeur	Exemple
Nom unique du composant DEM Orchestrator		Orchestrator-2
Nom unique du composant DEM Worker		Worker-1
Nom unique du composant DEM Worker		Worker-2
Nom unique du composant DEM Worker		Worker-3
Nom unique du composant DEM Worker		Worker-4

Configuration de votre équilibrage de charge

Après avoir déployé les dispositifs pour vRealize Automation, vous pouvez configurer un équilibrage de charge de façon à répartir le trafic entre plusieurs instances de dispositif vRealize Automation.

La liste suivante fournit une présentation des étapes générales requises pour configurer un équilibrage de charge pour le trafic vRealize Automation :

- 1 Installez votre équilibrage de charge
- 2 Activer l'affinité par session, également connue sous le nom de sessions sticky.
- 3 Assurez-vous que le délai d'expiration sur l'équilibrage de charge est d'au moins 100 secondes.
- 4 Si votre réseau ou votre équilibrage de charge l'exige, importez un certificat dans votre équilibrage de charge. Pour plus d'informations sur les relations de confiance et les certificats, reportez-vous à [Exigences de confiance du certificat dans un déploiement distribué](#). Pour plus d'informations sur l'extraction de certificats, reportez-vous à [Extraction de certificats et de clés privées](#).
- 5 Configurez l'équilibrage de charge pour le trafic dispositif vRealize Automation.
- 6 Configurez les dispositifs pour vRealize Automation. Reportez-vous à [Configuration de dispositifs pour vRealize Automation](#).

Note Lorsque vous configurez des dispositifs virtuels sous l'équilibrage de charge, faites-le uniquement pour les dispositifs virtuels qui ont été configurés pour être utilisés avec vRealize Automation. Si des dispositifs non configurés sont installés, des réponses erronées s'affichent.

Pour en savoir plus sur l'équilibrage de charge, consultez le livre blanc technique *Guide de configuration de l'équilibrage de charge de vRealize Automation*.

Pour obtenir des informations sur l'évolutivité et la haute disponibilité, reportez-vous au guide *Architecture de référence de vRealize Automation*.

Configuration de dispositifs pour vRealize Automation

Après avoir déployé vos dispositifs et configuré l'équilibrage de charge, vous configurez les dispositifs pour vRealize Automation.

Configurez le premier dispositif vRealize Automation dans un cluster

Le dispositif vRealize Automation est une machine virtuelle partiellement configurée qui héberge le serveur vRealize Automation et le portail Web d'utilisateur. Vous téléchargez et déployez le modèle OVF (Open Virtualization Format) vers vCenter Server ou l'inventaire ESX/ESXi.

Conditions préalables

- Créer un dispositif non configuré. Reportez-vous à [Déployer le dispositif vRealize Automation](#).
- Obtenez un certificat d'authentification pour le dispositif vRealize Automation.

Si votre réseau ou équilibrage de charge l'exige, les procédures ultérieures copient le certificat vers l'équilibrage de charge et des dispositifs supplémentaires.

Procédure

- 1 Connectez-vous à la nouvelle interface de gestion de dispositif vRealize Automation en tant qu'utilisateur racine.

`https://vrealize-automation-appliance-FQDN:5480`

Continuez après l'affichage éventuel des avertissements de certificat.
- 2 Si l'assistant d'installation s'affiche, annulez-le afin de pouvoir accéder à l'interface de gestion plutôt qu'à l'assistant.
- 3 Sélectionnez **Admin > Paramètres de l'heure** et définissez la source de synchronisation de l'heure.

Option	Description
Heure de l'hôte	Se synchroniser avec l'hôte ESXi du dispositif vRealize Automation.
Serveur de temps	Se synchroniser avec un serveur NTP (Network Time Protocol) externe. Entrez le nom de domaine complet ou l'adresse IP du serveur NTP.

Vous devez synchroniser tous les dispositifs vRealize Automation et serveurs IaaS Windows avec la même source de temps. Ne mélangez pas les sources de temps au sein d'un déploiement vRealize Automation.

4 Sélectionnez **vRA > Paramètres de l'hôte**.

Option	Action
Résoudre automatiquement	Sélectionnez Résoudre automatiquement pour spécifier le nom de l'hôte actuel du dispositif vRealize Automation.
Mise à jour de l'hôte	<p>Pour les nouveaux hôtes, sélectionnez Mise à jour de l'hôte. Entrez le nom de domaine complet du dispositif vRealize Automation, <i>vra-hostname.domain.name</i>, dans la zone de texte Nom d'hôte.</p> <p>Pour les déploiements distribués qui utilisent des équilibres de charge, sélectionnez Mise à jour de l'hôte. Entrez le nom de domaine complet du serveur d'équilibrage de charge, <i>vra-loadbalancename.domain.name</i>, dans la zone de texte Nom d'hôte.</p>

Note Configurez les paramètres SSO de la manière décrite plus loin dans cette procédure lorsque vous utilisez **Mise à jour de l'hôte** pour définir le nom d'hôte.

5 Sélectionnez l'action appropriée dans le menu **Action de certificat**.

Si vous utilisez un certificat codé au format PEM, pour un environnement distribué par exemple, sélectionnez **Importer**.

Les certificats que vous importez doivent être approuvés et être également applicables à toutes les instances de dispositif vRealize Automation et à tous les équilibres de charge par le biais de l'utilisation de certificats SAN (autre nom de l'objet).

Si vous souhaitez générer une demande CSR pour un nouveau certificat que vous pouvez envoyer à une autorité de certification, sélectionnez **Générer une demande de signature**. Une CSR permet à votre autorité de certification de créer un certificat avec les valeurs correctes que vous pouvez importer.

Note Si vous utilisez des chaînes de certificats, spécifiez les certificats dans l'ordre suivant :

- a Certificat client/serveur signé par le certificat CA intermédiaire
- b Un ou plusieurs certificats intermédiaires
- c Un certificat CA racine

Option	Action
Conserver l'existant	Conserver la configuration SSL actuelle. Sélectionnez cette option pour annuler vos modifications.
Générer un certificat	<ul style="list-style-type: none"> a La valeur affichée dans la zone de texte Nom commun est celle du nom d'hôte, tel qu'il s'affiche dans la partie supérieure de la page. Si des instances supplémentaires du dispositif vRealize Automation sont disponibles, leurs noms de domaine complets sont inclus dans l'attribut SAN du certificat. b Entrez le nom de votre organisation, comme le nom de votre société, dans la zone de texte Organisation. c Entrez votre unité d'organisation, comme le nom ou l'emplacement de votre service, dans la zone de texte Unité d'organisation. d Entrez un code pays ISO 3166, comme FR, dans la zone de texte Pays.

Option	Action
Générer une demande de signature	<ul style="list-style-type: none"> a Sélectionnez Générer une demande de signature. b Passez en revue les entrées dans les zones de texte Organisation, Unité d'organisation, Code du pays et Nom commun. Ces entrées sont remplies à partir du certificat existant. Vous pouvez modifier ces entrées si nécessaire. c Cliquez sur Générer une CSR pour générer un demande de signature de certificat, puis cliquez sur le lien Télécharger la demande CSR générée ici pour ouvrir une boîte de dialogue qui vous permet d'enregistrer la CSR à un emplacement d'où vous pouvez l'envoyer à une autorité de certification. d Lorsque vous recevez le certificat préparé, cliquez sur Importer et suivez les instructions permettant d'importer un certificat dans vRealize Automation.
Importer	<ul style="list-style-type: none"> a Copiez les valeurs du certificat de BEGIN PRIVATE KEY à END PRIVATE KEY, en incluant l'en-tête et le pied de page, et collez-les dans la zone de texte Clé privée RSA. b Copiez les valeurs du certificat de BEGIN CERTIFICATE à END CERTIFICATE, en incluant l'en-tête et le pied de page, dans la zone de texte Chaîne de certificat. Pour les valeurs de certificats multiples, incluez un en-tête BEGIN CERTIFICATE et un pied de page END CERTIFICATE pour chaque certificat. <hr/> <p>Note Dans le cas de certificats en chaînes, des attributs supplémentaires peuvent être disponibles.</p> <ul style="list-style-type: none"> c (Facultatif) Si votre certificat utilise une phrase secrète pour chiffrer la clé de certificat, copiez la phrase secrète et collez-la dans la zone de texte Phrase secrète.

6 Cliquez sur **Enregistrer les paramètres** pour enregistrer les informations de l'hôte et la configuration SSL.

7 Si requis par votre réseau ou votre équilibrage de charge, copiez le certificat importé ou nouvellement créé sur l'équilibrage de charge de dispositif virtuel.

Il se peut que vous deviez activer l'accès SSH racine afin d'exporter le certificat.

- a Si vous n'êtes pas déjà connecté, connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.

`https://vrealize-automation-appliance-FQDN:5480`

- b Cliquez sur l'onglet **Admin**.
- c Cliquez sur le sous-menu **Admin**.
- d Sélectionnez la case **Service SSH activé**.
Désélectionnez la case pour désactiver SSH une fois terminé.
- e Sélectionnez la case **Connexion SSH de l'administrateur**.
Désélectionnez la case pour désactiver SSH une fois terminé.
- f Cliquez sur **Enregistrer les paramètres**.

8 Configurez les paramètres SSO.**9** Cliquez sur **Services**.

Tous les services doivent être exécutés avant que vous puissiez installer une licence ou vous connecter à la console. Ils démarrent habituellement en 10 minutes environ.

Note Vous pouvez également vous connecter au dispositif et exécuter `tail -f /var/log/vcac/catalina.out` pour surveiller le démarrage du service.

10 Saisissez les informations sur votre licence.

- a Cliquez sur **vRA > Attribution de licence**.
- b Cliquez sur **Attribution de licence**.
- c Entrez une clé de licence vRealize Automation valide que vous avez téléchargée lors du téléchargement des fichiers d'installation, puis cliquez sur **Envoyer la clé**.

Note Si vous obtenez une erreur de connexion, l'équilibrage de charge peut présenter un problème. Vérifiez la connectivité réseau à l'équilibrage de charge.

11 Cliquez sur **Messagerie**. Les paramètres de configuration et l'état de la messagerie pour votre dispositif s'affichent. Ne modifiez pas ces paramètres.**12** Cliquez sur l'onglet **Télémétrie** pour indiquer si vous souhaitez participer au programme d'amélioration du produit de VMware (CEIP).

Pour en savoir plus sur les données collectées au titre du CEIP et leur utilisation par VMware, consultez le Trust & Assurance Center à l'adresse <http://www.vmware.com/trustvmware/ceip.html>.

- Cochez la case **Rejoindre le programme d'amélioration du produit de VMware** pour participer au programme.
- Désactivez la case **Rejoindre le programme d'amélioration du produit de VMware** pour ne pas participer au programme.

13 Cliquez sur **Enregistrer les paramètres**.**14** Vérifiez que vous pouvez vous connecter à vRealize Automation.

- a Ouvrez un navigateur Web et accédez à l'URL de l'interface produit de vRealize Automation.

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

- b Si vous y êtes invité, poursuivez après les avertissements de certificat.
- c Connectez-vous avec l'identifiant `administrator@vsphere.local` et le mot de passe que vous avez spécifié lorsque vous avez configuré SSO.

L'interface s'ouvre sur la page Locataires dans l'onglet **Administration**. Un locataire nommé `vsphere.local` figure dans la liste.

Configuration d'instances supplémentaires du dispositif vRealize Automation

L'administrateur système peut déployer plusieurs instances du dispositif vRealize Automation afin d'assurer la redondance dans un environnement à haute disponibilité.

Pour chaque dispositif vRealize Automation, vous devez activer la synchronisation de l'heure et ajouter le dispositif à un cluster. Les informations de configuration basées sur les paramètres du dispositif vRealize Automation (principal) initial sont ajoutées automatiquement lorsque vous ajoutez le dispositif au cluster.

Si vous effectuez une installation distribuée avec équilibrages de charge pour la haute disponibilité et le basculement, informez le responsable d'équipe pour qu'il configure votre environnement vRealize Automation. Vos administrateurs de locataires doivent configurer la fonctionnalité Gestion des annuaires en vue de la haute disponibilité lorsqu'ils configurent le lien vers votre Active Directory.

Ajouter un autre dispositif vRealize Automation au cluster

Pour la haute disponibilité, des installations distribuées peuvent utiliser un équilibrage de charge devant un cluster de nœuds de dispositifs vRealize Automation.

Vous utilisez l'interface de gestion sur le nouveau dispositif vRealize Automation pour le joindre à un cluster existant d'un ou de plusieurs dispositifs. L'opération de jonction copie les informations de configuration dans le nouveau dispositif que vous ajoutez, notamment des informations sur les certificats, SSO, les licences, la base de données et la messagerie.

Active Directory—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. Après avoir ajouté un autre dispositif, n'oubliez pas de configurer un second connecteur qui correspond au dispositif ajouté. Le second connecteur se connecte à votre fournisseur d'identité et pointe vers le même dispositif Active Directory. De cette manière, si le premier dispositif échoue, le second prend en charge la gestion de l'authentification de l'utilisateur.

Vous devez ajouter les dispositifs à un cluster un à la fois et non en parallèle.

Conditions préalables

- Un ou plusieurs dispositifs vRealize Automation doivent être prêts dans le cluster, dont l'un d'entre eux est le nœud principal. Reportez-vous à [Configurez le premier dispositif vRealize Automation dans un cluster](#).

Vous pouvez désigner un nouveau dispositif comme nœud principal uniquement après l'avoir joint au cluster.

- Créez le nouveau nœud de dispositif. Reportez-vous à [Déployer le dispositif vRealize Automation](#).
- Vérifiez que l'équilibrage de charge est configuré pour une utilisation avec le nouveau dispositif.

- Vérifiez que le trafic peut franchir l'équilibrage de charge pour atteindre tous les nœuds actuels ainsi que le nouveau nœud que vous allez ajouter.
- Vérifiez que tous les services vRealize Automation sont démarrés sur les nœuds en cours.

Procédure

- 1 Connectez-vous à la nouvelle interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.

`https://vrealize-automation-appliance-FQDN:5480`

Continuez après l'affichage éventuel des avertissements de certificat.
- 2 Si l'assistant d'installation s'affiche, annulez-le afin de pouvoir accéder à l'interface de gestion plutôt qu'à l'assistant.
- 3 Sélectionnez **Admin > Paramètres de l'heure** et définissez la source de temps sur celle que le reste des dispositifs du cluster utilisent.
- 4 Sélectionnez **vRA > Cluster**.
- 5 Entrez le nom de domaine complet d'un dispositif vRealize Automation configuré précédemment dans la zone de texte **Nœud de cluster de début**.

Vous pouvez utiliser le nom de domaine complet du dispositif vRealize Automation principal ou de tout dispositif vRealize Automation déjà associé au cluster.
- 6 Tapez le mot de passe racine dans la zone de texte **Mot de passe**.
- 7 Cliquez sur **Joindre un cluster**.
- 8 Continuez après l'affichage éventuel des avertissements de certificat.

Les services du cluster sont redémarrés.
- 9 Vérifiez que les services sont en cours d'exécution.
 - a Cliquez sur l'onglet **Services**.
 - b Cliquez sur l'onglet **Actualiser** pour suivre la progression du démarrage des services.

Résultats

Si une opération Joindre un cluster prend un certain temps et finit par expirer, reportez-vous à [l'article 58708 de la Base de connaissances VMware](#).

Désactiver les services inutilisés

Pour conserver des ressources internes en cas d'utilisation d'une instance externe de vRealize Orchestrator, vous pouvez désactiver le service vRealize Orchestrator intégré.

Conditions préalables

[Ajouter un autre dispositif vRealize Automation au cluster](#)

Procédure

- 1 Connectez-vous à la console du dispositif vRealize Automation.
- 2 Arrêtez le service vRealize Orchestrator.

```
service vco-server stop
chkconfig vco-server off
```

Valider le déploiement distribué

Après avoir déployé des instances supplémentaires du dispositif vRealize Automation, vous confirmez que vous pouvez accéder aux dispositifs en cluster.

Procédure

- 1 Dans l'interface de gestion d'équilibrage de charge ou le fichier de configuration, désactivez temporairement tous les nœuds, sauf le nœud que vous testez.
- 2 Confirmez que vous pouvez vous connecter à vRealize Automation via l'adresse de l'équilibrage de charge :

`https://vrealize-automation-appliance-load-balancer-FQDN/vcac`
- 3 Après avoir vérifié que vous pouvez accéder au nouveau dispositif vRealize Automation via l'équilibrage de charge, réactivez les autres nœuds.

Installer les composants IaaS dans une configuration distribuée

L'administrateur système installe les composants IaaS une fois que les dispositifs sont déployés et entièrement configurés. Les composants IaaS fournissent l'accès aux fonctionnalités de l'infrastructure vRealize Automation.

Tous les composants doivent s'exécuter sous le même utilisateur de compte de service, qui doit être un compte de domaine ayant des privilèges sur chaque serveur IaaS distribuer. N'utilisez pas de comptes système locaux.

Conditions préalables

- [Configurez le premier dispositif vRealize Automation dans un cluster.](#)
- Si votre site inclut plusieurs dispositifs vRealize Automation, [Ajouter un autre dispositif vRealize Automation au cluster.](#)
- Vérifiez que le serveur répond aux exigences dans la section [Serveurs Windows IaaS.](#)
- Obtenez un certificat auprès d'une autorité de certification approuvée pour l'importation dans le magasin de certificats root approuvés des machines sur lesquels vous prévoyez d'installer le site Web du composant et Model Manager Data.

- Si vous utilisez des équilibres de charge dans votre environnement, vérifiez qu'ils correspondent aux exigences de configuration.

Procédure

1 Installer des certificats IaaS

Pour les environnements de production, obtenez un certificat de domaine auprès d'une autorité de certification de confiance. Importez le certificat dans le magasin de certificats racines approuvés de toutes les machines sur lesquelles vous prévoyez d'installer le composant de site Web et Manager Service (les machines IIS) lors de l'installation d'IaaS.

2 Télécharger le programme d'installation de vRealize Automation IaaS

Pour installer IaaS sur vos serveurs Windows distribués virtuels ou physiques, vous téléchargez une copie du programme d'installation d'IaaS à partir du dispositif vRealize Automation.

3 Choisir un scénario de base de données IaaS

vRealize Automation IaaS utilise une base de données Microsoft SQL Server pour conserver les informations relatives aux machines qu'il gère et ses propres éléments et stratégies.

4 Installer un composant de site Web IaaS et Model Manager Data

L'administrateur système installe le composant de site Web pour fournir accès aux capacités de l'infrastructure de la console Web vRealize Automation. Vous pouvez installer une ou plusieurs instances du composant de site Web, mais vous devez configurer le composant Model Manager Data sur la machine hébergeant le premier composant de site Web. Vous n'installez Model Manager Data qu'une seule fois.

5 Installer des composants de serveur Web IaaS supplémentaires

Le serveur Web donne accès à des fonctionnalités d'infrastructure dans vRealize Automation. Une fois le premier serveur Web installé, vous pouvez augmenter les performances en installant des serveurs Web IaaS supplémentaires.

6 Installer le service Active Manager Service

Le composant Manager Service actif est un service Windows qui coordonne la communication entre les instances de IaaS Distributed Execution Manager, la base de données, les agents, les agents proxy et SMTP.

7 Installer un composant de sauvegarde Manager Service

Le service de sauvegarde Manager Service assure la redondance et la haute disponibilité, et peut être démarré manuellement si le service actif s'arrête.

8 Installation des composants Distributed Execution Manager

Vous installez le DEM en tant que l'un des rôles : DEM Orchestrator ou DEM Worker. Vous devez installer au moins une instance de DEM pour chaque rôle et vous pouvez installer des instances de DEM supplémentaires pour prendre en charge le basculement et la haute disponibilité.

9 Configuration du service Windows pour accéder à la base de données IaaS

Un administrateur système peut modifier la méthode d'authentification utilisée pour accéder à la base de données SQL lors de l'exécution (une fois l'installation terminée). Par défaut, l'identité Windows du compte actuellement connecté est utilisée pour connecter la base de données une fois son installation terminée.

10 Vérifier les services IaaS

Après l'installation, l'administrateur système vérifie que les services IaaS sont en cours d'exécution. Si c'est bien le cas, l'installation est réussie.

Étape suivante

Installez une instance de DEM Orchestrator et au moins une instance de DEM Worker. Reportez-vous à [Installation des composants Distributed Execution Manager](#).

Installer des certificats IaaS

Pour les environnements de production, obtenez un certificat de domaine auprès d'une autorité de certification de confiance. Importez le certificat dans le magasin de certificats racines approuvés de toutes les machines sur lesquelles vous prévoyez d'installer le composant de site Web et Manager Service (les machines IIS) lors de l'installation d'IaaS.

Conditions préalables

Sur les machines Windows 2012, vous devez désactiver TLS1.2 pour les certificats qui utilisent SHA512. Pour en savoir plus sur la désactivation de TLS1.2, consultez [Article 245030 de la base de connaissances Microsoft](#).

Procédure

- 1 Obtenez un certificat auprès d'une autorité de certification de confiance.
- 2 Ouvrez le Gestionnaire des services Internet Information Services IIS.
- 3 Dans la vue Fonctionnalités, double-cliquez sur **Certificats de serveur**.
- 4 Dans le volet Actions, cliquez sur **Importer**.
 - a Entrez un nom de fichier dans la zone de texte **Fichier de certificat** ou cliquez sur le bouton Parcourir (...) pour accéder au nom d'un fichier où le certificat exporté est stocké.
 - b Si le certificat a été exporté avec un mot de passe, entrez le mot de passe dans la zone de texte **Mot de passe**.
 - c Sélectionnez **Marquer cette clé comme exportable**.
- 5 Cliquez sur **OK**.
- 6 Cliquez sur le certificat importé et sélectionnez **Afficher**.

- 7 Vérifiez que le certificat et sa chaîne sont approuvés.

Si le certificat est non approuvé, le message `Ce certificat racine de l'Autorité de certification n'est pas de confiance` s'affiche.

Note Vous devez résoudre le problème de confiance avant de procéder à l'installation. Si vous continuez, votre déploiement échoue.

- 8 Redémarrez IIS, ouvrez une fenêtre d'invite de commande élevée et tapez `iisreset`.

Étape suivante

[Télécharger le programme d'installation de vRealize AutomationlaaS.](#)

Télécharger le programme d'installation de vRealize AutomationlaaS

Pour installer laaS sur vos serveurs Windows distribués virtuels ou physiques, vous téléchargez une copie du programme d'installation d'laaS à partir du dispositif vRealize Automation.

Si des avertissements de certificat s'affichent pendant ce processus, continuez après ces avertissements pour terminer l'installation.

Conditions préalables

- [Configurez le premier dispositif vRealize Automation dans un cluster](#) et, éventuellement, [Ajouter un autre dispositif vRealize Automation au cluster](#).
- Vérifiez que le serveur répond aux exigences dans la section [Serveurs Windows laaS](#).
- Vérifiez que vous avez installé un certificat pour IIS et que la racine du certificat ou l'autorité de certification se trouve dans la racine de confiance sur la machine d'installation.
- Si vous utilisez des équilibres de charge dans votre environnement, vérifiez qu'ils correspondent aux exigences de configuration.

Procédure

- 1 (Facultatif) Activez HTTP si vous procédez à l'installation sur une machine Windows 2012.
 - a Sélectionnez **Fonctionnalités > Ajouter des fonctionnalités** depuis Server Manager.
 - b Développez **Services WCF** sous Fonctionnalités .NET Framework.
 - c Sélectionnez **Activation HTTP**.
- 2 Connectez-vous au serveur laaS Windows en utilisant un compte ayant des droits d'administrateur.
- 3 Ouvrez un navigateur Web directement à l'URL du programme d'installation du dispositif vRealize Automation. N'utilisez pas d'adresse d'équilibrage de charge.

<https://vrealize-automation-appliance-FQDN:5480/installer>
- 4 Cliquez sur **Programme d'installation d'laaS**.

- 5 Enregistrez `setup__vrealize-automation-appliance-FQDN@5480` sur le serveur Windows.

Ne modifiez pas le nom de fichier du programme d'installation. Il est utilisé pour connecter l'installation au dispositif vRealize Automation

- 6 Téléchargez le fichier du programme d'installation sur tous les serveurs Windows IaaS sur lesquels vous installez des composants.

Étape suivante

Installez une base de données IaaS, reportez-vous à [Choisir un scénario de base de données IaaS](#).

Choisir un scénario de base de données IaaS

vRealize Automation IaaS utilise une base de données Microsoft SQL Server pour conserver les informations relatives aux machines qu'il gère et ses propres éléments et stratégies.

En fonction de vos préférences et privilèges, vous pouvez choisir parmi plusieurs procédures pour créer la base de données IaaS.

Note Vous pouvez activer la base de données SSL sécurisée lorsque vous créez ou mettez à niveau la base de données SQL. Par exemple, lorsque vous créez ou mettez à niveau la base de données SQL, vous pouvez utiliser l'option SSL sécurisé pour demander que la configuration SSL déjà définie dans le serveur SQL soit appliquée lors de la connexion à la base de données SQL. SSL fournit une connexion plus sécurisée entre le serveur IaaS et la base de données SQL. Cette option, qui est disponible dans l'assistant d'installation personnalisé, nécessite d'avoir déjà configuré SSL sur le serveur SQL. Pour en savoir plus sur la configuration de SSL sur SQL Server, consultez [Article 189067 de Microsoft Technet](#).

Tableau 5-7. Choisir un scénario de base de données IaaS

Scénario	Procédure
Créez la base de données IaaS manuellement à l'aide des scripts fournis pour la base de données. Cette option permet à un administrateur de base de données de vérifier les modifications avec soin avant de créer la base de données.	Créer la base de données IaaS manuellement.
Préparez une base de données vide et utilisez le programme d'installation pour remplir le schéma de base de données. Cette option permet au programme d'installation d'utiliser un utilisateur de base de données avec des privilèges dbo pour remplir la base de données.	Préparer une base de données vide .
Utilisez le programme d'installation pour créer la base de données. Cette option est la plus simple mais requiert l'utilisation de privilèges sysadmin dans le programme d'installation.	Créer la base de données IaaS à l'aide de l'assistant d'installation.

Créer la base de données IaaS manuellement

L'administrateur système de vRealize Automation peut créer la base de données manuellement à l'aide des scripts fournis par VMware.

Conditions préalables

- Installez Microsoft .NET Framework 4.5.2 ou version ultérieure sur l'hôte SQL Server.
- Pour vous connecter à la base de données, utilisez l'authentification Windows au lieu de l'authentification SQL.
- Vérifiez la configuration requise pour l'installation de la base de données. Reportez-vous à [Hôte du serveur SQL IaaS](#).
- Ouvrez un navigateur Web à l'URL du programme d'installation de dispositif vRealize Automation, puis téléchargez les scripts d'installation de la base de données IaaS.

<https://vrealize-automation-appliance-FQDN:5480/installer>

Procédure

- 1 Accédez au sous-répertoire Base de données dans le répertoire où vous avez extrait l'archive zip d'installation.
- 2 Extrayez l'archive DBInstall.zip dans un répertoire local.
- 3 Connectez-vous à l'hôte de base de données Windows avec des droits suffisants pour créer et déposer des privilèges **sysadmin** dans l'instance SQL Server.
- 4 Vérifiez les scripts de déploiement de la base de données selon vos besoins. En particulier, vérifiez les paramètres dans la section DBSettings du fichier CreateDatabase.sql et modifiez-les si nécessaire.

Les paramètres dans le script sont les paramètres recommandés. Seuls les paramètres ALLOW_SNAPSHOT_ISOLATION ON et READ_COMMITTED_SNAPSHOT ON sont obligatoires.

- 5 Exécutez la commande suivante avec les arguments décrits dans le tableau.

```
BuildDB.bat /p:DBServer=db_server;
DBName=db_name;DBDir=db_dir;
LogDir=[log_dir];ServiceUser=service_user;
ReportLogin=web_user;
VersionString=version_string
```

Tableau 5-8. Valeurs de la base de données

Variable	Valeur
<i>db_server</i>	Spécifie l'instance SQL Server dans le format <code>dbhostname[,port number]\SQL instance</code> . Spécifiez un numéro de port uniquement si vous n'utilisez pas le port par défaut. Le numéro de port Microsoft SQL par défaut est 1433. La valeur par défaut pour <i>db_server</i> est <code>localhost</code> .
<i>db_name</i>	Nom de la base de données. La valeur par défaut est <code>vra</code> . Les noms de base de données ne doivent pas contenir plus de 128 caractères ASCII.
<i>db_dir</i>	Chemin vers le répertoire de données de la base de données, en excluant la barre oblique finale.
<i>log_dir</i>	Chemin vers le répertoire de journaux de la base de données, en excluant la barre oblique finale.
<i>service_user</i>	Nom d'utilisateur utilisé pour exécuter Manager Service.
<i>Web_user</i>	Nom d'utilisateur utilisé pour exécuter les services Web.
<i>version_string</i>	Version de vRealize Automation, trouvée en se connectant au dispositif vRealize Automation et en cliquant dans l'onglet Mettre à jour. Par exemple, la chaîne de la version 6.1 de vRealize Automation est <code>6.1.0.1200</code> .

Résultats

La base de données a été créée.

Étape suivante

[Installer les composants IaaS dans une configuration distribuée.](#)

Préparer une base de données vide

Un administrateur système de vRealize Automation peut installer le schéma IaaS sur une base de données vide. Cette méthode d'installation offre un contrôle maximal sur la sécurité de la base de données.

Conditions préalables

- Vérifiez la configuration requise pour l'installation de la base de données. Reportez-vous à [Hôte du serveur SQL IaaS](#).
- Ouvrez un navigateur Web à l'URL du programme d'installation de dispositif vRealize Automation, puis téléchargez les scripts d'installation de la base de données IaaS.

`https://vrealize-automation-appliance-FQDN:5480/installer`

Procédure

- 1 Accédez au répertoire Base de données situé dans le répertoire où vous avez extrait le fichier d'installation compressé (zip).
- 2 Extrayez l'archive DBInstall.zip dans un répertoire local.
- 3 Connectez-vous à l'hôte de la base de données Windows avec des privilèges **administrateur système** dans l'instance du serveur SQL Server.
- 4 Modifiez les fichiers suivants et remplacez toutes les instances des variables du tableau par les valeurs correctes pour votre environnement.

```
CreateDatabase.sql
SetDatabaseSettings.sql
```

Tableau 5-9. Valeurs de la base de données

Variable	Valeur
\$(DBName)	Nom de la base de données, comme vra. Les noms de base de données ne doivent pas contenir plus de 128 caractères ASCII.
\$(DBDir)	Chemin vers le répertoire de données de la base de données, en excluant la barre oblique finale.
\$(LogDir)	Chemin vers le répertoire de journaux de la base de données, en excluant la barre oblique finale.

- 5 Vérifiez les paramètres dans la section Paramètres de la base de données de SetDatabaseSettings.sql et modifiez-les au besoin.

Les paramètres du script correspondent aux paramètres recommandés pour la base de données IaaS. Seuls ALLOW_SNAPSHOT_ISOLATION ON et READ_COMMITTED_SNAPSHOT ON sont requis.

- 6 Ouvrez SQL Server Management Studio.
- 7 Cliquez sur **Nouvelle requête**.
Une fenêtre Requête SQL s'ouvre.
- 8 Dans le menu **Requête**, vérifiez que **Mode SQLCMD** est sélectionné.
- 9 Collez tout le contenu modifié de CreateDatabase.sql dans le panneau de la requête.
- 10 Sous le contenu de CreateDatabase.sql, collez tout le contenu modifié de SetDatabaseSettings.sql.
- 11 Cliquez sur **Exécuter**.
Le script s'exécute et crée la base de données.

Étape suivante

[Installer les composants IaaS dans une configuration distribuée.](#)

Créer la base de données IaaS à l'aide de l'assistant d'installation

vRealize Automation utilise une base de données Microsoft SQL Server pour mettre à jour les informations sur les machines qu'il gère et ses propres éléments et stratégies.

La procédure suivante décrit comment créer la base de données IaaS à l'aide du programme d'installation ou compléter une base de données vide. Il est également possible de créer la base de données manuellement. Reportez-vous à [Créer la base de données IaaS manuellement](#).

Conditions préalables

- Si vous créez la base de données avec l'authentification Windows au lieu de l'authentification SQL, vérifiez que l'utilisateur qui exécute le programme d'installation dispose des droits **sysadmin** sur le serveur SQL.
- [Télécharger le programme d'installation de vRealize Automation IaaS](#).

Procédure

- 1 Cliquez avec le bouton droit sur le fichier d'installation `setup__vrealize-automation-appliance-FQDN@5480.exe` et sélectionnez **Exécuter en tant qu'administrateur**.
- 2 Cliquez sur **Suivant**.
- 3 Acceptez le contrat de licence, puis cliquez sur **Suivant**.
- 4 Sur la page de connexion, fournissez les informations d'identification d'administrateur pour le dispositif vRealize Automation et vérifiez le certificat SSL.
 - a Entrez le nom d'utilisateur **root** et le mot de passe.
Le mot de passe est celui que vous avez spécifié lors du déploiement du dispositif vRealize Automation.
 - b Sélectionnez **Accepter le certificat**.
 - c Cliquez sur **Afficher le certificat**.
Comparez l'empreinte de certificat à l'empreinte définie pour le dispositif vRealize Automation. Vous pouvez afficher le certificat du dispositif vRealize Automation dans le navigateur du client si vous avez accédé à l'interface de gestion du dispositif vRealize Automation sur le port 5480.
- 5 Cliquez sur **Suivant**.
- 6 Sur la page Type d'installation, sélectionnez **Installation personnalisée**.
- 7 Dans la section Composant sur la page Type d'installation, sélectionnez **Serveur IaaS**.
- 8 Acceptez l'emplacement d'installation racine ou cliquez sur **Modifier** et sélectionnez le chemin d'installation.

Même dans un déploiement distribué, vous pouvez être amené à installer plusieurs composants IaaS sur un même serveur Windows.

Si vous installez plusieurs composants IaaS, veillez toujours à les installer au même endroit.

- 9 Cliquez sur **Suivant**.
- 10 Sur la page d'installation personnalisée du serveur IaaS, sélectionnez **Base de données**.
- 11 Dans la zone de texte **Instance de base de données**, spécifiez l'instance de base de données ou cliquez sur **Rechercher** et sélectionnez-la dans la liste des instances. Si l'instance de base de données n'est pas un port par défaut, incluez le numéro du port dans la spécification de l'instance en utilisant le formulaire `dbhost,SQL_port_number\SQLinstance`. Le numéro de port par défaut Microsoft SQL est 1443.
- 12 (Facultatif) Cochez la case **Utiliser SSL pour la connexion à la base de données**.
 Par défaut, la case est activée. SSL fournit une connexion plus sécurisée entre le serveur IaaS et la base de données SQL. Néanmoins, vous devez d'abord configurer le protocole SSL sur le serveur SQL pour prendre en charge cette option. Pour obtenir plus d'informations sur la configuration de SSL sur SQL Server, consultez [Article 189067 de Microsoft Technet](#).
- 13 Sélectionnez le type d'installation de base de données dans le volet **Nom de la base de données**.
 - Pour créer le schéma dans une base de données existante, sélectionnez **Utiliser une base de données vide existante**.
 - Pour créer une nouvelle base de données, saisissez un nouveau nom de base de données ou utilisez le nom par défaut **vra**. Les noms de base de données ne doivent pas contenir plus de 128 caractères ASCII.
- 14 Pour spécifier d'autres emplacements, décochez l'option **Utiliser les répertoires de données et de journaux par défaut** ou laissez cette option sélectionnée pour utiliser les répertoires par défaut (recommandé).
- 15 Sélectionnez le mode d'authentification pour l'installation de la base de données dans la liste **Authentification**.
 - Pour utiliser les informations d'identification avec lesquelles vous exécutez le programme d'installation pour créer la base de données, sélectionnez **Utiliser identité Windows...**
 - Pour utiliser l'authentification SQL, décochez l'option **Utiliser identité Windows...** Entrez les informations d'identification SQL dans les zones de texte Utilisateur et Mot de passe.

Par défaut, le compte d'utilisateur du service Windows est utilisé lors de l'accès d'exécution à la base de données, qui doit disposer des droits sysadmin d'accès à l'instance SQL Server. Les informations d'identification utilisées pour accéder à la base de données peuvent être configurées pour utiliser les informations d'identification SQL.

L'authentification Windows est recommandée. Lorsque vous choisissez l'authentification SQL, le mot de passe de la base de données non chiffré figure dans certains fichiers de configuration.
- 16 Cliquez sur **Suivant**.

17 Terminez la vérification des conditions préalables.

Option	Description
Aucune erreur	Cliquez sur Suivant .
Erreurs non critiques	Cliquez sur Aucune correction .
Erreurs critiques	Si vous ne corrigez pas les erreurs critiques, l'installation échoue. Si des avertissements s'affichent, sélectionnez l'avertissement dans le volet gauche et suivez les instructions à droite. Résolvez toutes les erreurs critiques et cliquez sur Vérifier à nouveau pour vérifier.

18 Cliquez sur **Installer**.**19** Lorsque le message de réussite s'affiche, décochez l'option **Me guider dans la configuration initiale** et cliquez sur **Suivant**.**20** Cliquez sur **Terminer**.**Résultats**

La base de données est prête à être utilisée.

Installer un composant de site Web IaaS et Model Manager Data

L'administrateur système installe le composant de site Web pour fournir accès aux capacités de l'infrastructure de la console Web vRealize Automation. Vous pouvez installer une ou plusieurs instances du composant de site Web, mais vous devez configurer le composant Model Manager Data sur la machine hébergeant le premier composant de site Web. Vous n'installez Model Manager Data qu'une seule fois.

Conditions préalables

- Installez la base de données IaaS. Pour cela, reportez-vous à la section [Choisir un scénario de base de données IaaS](#).
- Si vous avez installé déjà d'autres composants IaaS, vous devez connaître la phrase secrète de la base de données que vous avez créée.
- Si vous utilisez des équilibres de charge dans votre environnement, vérifiez qu'ils correspondent aux exigences de configuration.

Procédure**1** [Installer le premier composant de serveur Web IaaS](#)

Vous installez le composant de serveur Web IaaS pour donner accès aux fonctionnalités d'infrastructure de vRealize Automation.

2 [Configurer Model Manager Data](#)

Vous installez le composant Model Manager sur la machine qui héberge le premier composant du serveur Web. Vous n'installez Model Manager Data qu'une seule fois.

Résultats

Vous pouvez installer des composants supplémentaires du site Web ou installer le service Manager. Reportez-vous à la section [Installer des composants de serveur Web IaaS supplémentaires](#) ou [Installer le service Active Manager Service](#).

Installer le premier composant de serveur Web IaaS

Vous installez le composant de serveur Web IaaS pour donner accès aux fonctionnalités d'infrastructure de vRealize Automation.

Vous pouvez installer plusieurs serveurs Web IaaS, mais uniquement le premier inclut Model Manager Data.

Conditions préalables

- [Créer la base de données IaaS à l'aide de l'assistant d'installation.](#)
- Vérifiez que le serveur répond aux exigences dans la section [Serveurs Windows IaaS](#).
- Si vous avez installé déjà d'autres composants IaaS, vous devez connaître la phrase secrète de la base de données que vous avez créée.
- Si vous utilisez des équilibres de charge dans votre environnement, vérifiez qu'ils correspondent aux exigences de configuration.

Procédure

- 1 Si vous utilisez un équilibre de charge, désactivez les autres nœuds sous l'équilibre de charge, puis vérifiez que le trafic est redirigé vers le nœud souhaité.
En outre, désactivez les contrôles de santé de l'équilibre de charge jusqu'à ce que tous les composants vRealize Automation aient été installés et configurés.
- 2 Cliquez avec le bouton droit sur le fichier d'installation `setup__vrealize-automation-appliance-FQDN@5480.exe` et sélectionnez **Exécuter en tant qu'administrateur**.
- 3 Cliquez sur **Suivant**.
- 4 Acceptez le contrat de licence, puis cliquez sur **Suivant**.

- 5 Sur la page de connexion, fournissez les informations d'identification d'administrateur pour le dispositif vRealize Automation et vérifiez le certificat SSL.

- a Entrez le nom d'utilisateur **root** et le mot de passe.

Le mot de passe est celui que vous avez spécifié lors du déploiement du dispositif vRealize Automation.

- b Sélectionnez **Accepter le certificat**.

- c Cliquez sur **Afficher le certificat**.

Comparez l'empreinte de certificat à l'empreinte définie pour le dispositif vRealize Automation. Vous pouvez afficher le certificat du dispositif vRealize Automation dans le navigateur du client si vous avez accédé à l'interface de gestion du dispositif vRealize Automation sur le port 5480.

- 6 Cliquez sur **Suivant**.

- 7 Sur la page Type d'installation, sélectionnez **Installation personnalisée**.

- 8 Dans la section Composant sur la page Type d'installation, sélectionnez **Serveur IaaS**.

- 9 Acceptez l'emplacement d'installation racine ou cliquez sur **Modifier** et sélectionnez le chemin d'installation.

Même dans un déploiement distribué, vous pouvez être amené à installer plusieurs composants IaaS sur un même serveur Windows.

Si vous installez plusieurs composants IaaS, veillez toujours à les installer au même endroit.

- 10 Cliquez sur **Suivant**.

- 11 Sélectionnez **Site Web** et **Données Model Manager** sur la page **Installation personnalisée du serveur IaaS**.

- 12 Sélectionnez un site Web parmi ceux qui sont disponibles ou acceptez le site Web par défaut dans l'onglet **Site Web Administration et Model Manager**.

- 13 Entrez un numéro de port disponible dans la zone de texte **Numéro de port** ou acceptez le port par défaut 443.

- 14 Cliquez sur **Tester la liaison** pour confirmer que le numéro de port est disponible.

- 15 Sélectionnez le certificat pour ce composant.

- a Si vous avez importé un certificat après avoir commencé l'installation, cliquez sur **Actualiser** pour mettre la liste à jour.

- b Sélectionnez le certificat à utiliser dans la section **Certificats disponibles**.

- c Si vous avez importé un certificat qui n'a pas de nom convivial et qui n'apparaît pas dans la liste, désélectionnez l'option **Afficher les certificats utilisant des noms conviviaux** et cliquez sur **Actualiser**.

Si vous effectuez l'installation dans un environnement qui n'utilise pas d'équilibrages de charge, vous pouvez sélectionner **Générer un certificat auto-signé** au lieu de sélectionner un

certificat. Si vous installez des composants de site Web supplémentaires derrière un équilibrage de charge, ne générez pas de certificats auto-signés. Pour garantir que vous utilisez le même certificat sur tous les serveurs derrière l'équilibrage de charge, importez le certificat depuis le serveur Web IaaS principal.

- 16 (Facultatif) Cliquez sur **Afficher le certificat**, affichez le certificat et cliquez sur **OK** pour fermer la fenêtre d'information.
- 17 (Facultatif) Sélectionnez **Supprimer les incompatibilités de certificat** pour supprimer les erreurs de certificat. L'installation ignore les erreurs d'incompatibilité de nom de certificat et toutes les erreurs de correspondance de liste à distance de révocation de certificat.

Il s'agit d'une option moins sécurisée.

Configurer Model Manager Data

Vous installez le composant Model Manager sur la machine qui héberge le premier composant du serveur Web. Vous n'installez Model Manager Data qu'une seule fois.

Conditions préalables

[Installer le premier composant de serveur Web IaaS.](#)

Procédure

- 1 Cliquez sur l'onglet **Model Manager Data**.
- 2 Dans la zone de texte **Serveur**, entrez le nom de domaine complet du dispositif vRealize Automation.
vrealize-automation-appliance.mycompany.com
N'entrez pas d'adresse IP.
- 3 Cliquez sur **Charger** pour afficher le **Locataire SSO par défaut**.
Le locataire par défaut `vsphere.local` est créé automatiquement lorsque vous configurez single sign-on. Ne le modifiez pas.
- 4 Cliquez sur **Télécharger** pour importer le certificat à partir du dispositif virtuel.
Le téléchargement du certificat peut prendre quelques minutes.
- 5 (Facultatif) Cliquez sur **Afficher le certificat**, affichez le certificat et cliquez sur **OK** pour fermer la fenêtre d'information.
- 6 Cliquez sur **Accepter le certificat**.
- 7 Entrez `administrator@vsphere.local` dans la zone de texte **Nom d'utilisateur** et entrez le mot de passe que vous avez créé lorsque vous avez configuré SSO dans les zones de texte **Mot de passe** et **Confirmer**.
- 8 (Facultatif) Cliquez sur **Tester** pour vérifier les informations d'identification.

- 9 Dans la zone de texte **Serveur IaaS**, identifiez le composant de serveur Web IaaS.

Option	Description
Avec équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant de serveur Web IaaS, <i>web-load-balancer.mycompany.com:443</i> . N'entrez pas d'adresses IP.
Sans équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de la machine sur laquelle vous avez installé le composant de serveur Web IaaS, <i>web.mycompany.com:443</i> . N'entrez pas d'adresses IP.

Le port par défaut est 443.

- 10 Cliquez sur **Tester** pour vérifier la connexion du serveur.
- 11 Cliquez sur **Suivant**.
- 12 Terminez la vérification des conditions préalables.

Option	Description
Aucune erreur	Cliquez sur Suivant .
Erreurs non critiques	Cliquez sur Aucune correction .
Erreurs critiques	Si vous ne corrigez pas les erreurs critiques, l'installation échoue. Si des avertissements s'affichent, sélectionnez l'avertissement dans le volet gauche et suivez les instructions à droite. Résolvez toutes les erreurs critiques et cliquez sur Vérifier à nouveau pour vérifier.

- 13 Sur la page Paramètres de serveur et de compte, dans les zones de texte **Informations d'installation du serveur**, entrez le nom d'utilisateur et le mot de passe de l'utilisateur du compte de service ayant des privilèges administratifs sur le serveur d'installation actuel.

L'utilisateur du compte de service doit correspondre à un compte de domaine ayant des privilèges sur chaque serveur IaaS distribué. N'utilisez pas de comptes système locaux.

- 14 Fournissez la phrase secrète utilisée pour générer la clé de chiffrement qui protège la base de données.

Option	Description
Si vous avez déjà installé des composants dans cet environnement	Entrez la phrase secrète créée auparavant dans les zones de texte Phrase secrète et Confirmer .
S'il s'agit de la première installation	Entrez une phrase secrète dans les zones de texte Phrase secrète et Confirmer . Vous devez utiliser cette phrase secrète à chaque fois que vous installez un nouveau composant.

Conservez cette phrase secrète dans un lieu sûr pour l'utiliser ultérieurement.

- 15** Spécifiez le serveur de base de données IaaS, le nom de la base de données et la méthode d'authentification pour le serveur de base de données dans la zone de texte **Informations d'installation de la base de données Microsoft SQL**.

Il s'agit du serveur de base de données, du nom et des informations d'authentification que vous avez créés auparavant.

- 16** Cliquez sur **Suivant**.

- 17** Cliquez sur **Installer**.

- 18** Lorsque l'installation est terminée, désélectionnez **Me guider tout au long de la configuration initiale** et cliquez sur **Suivant**.

Étape suivante

Vous pouvez installer des composants de serveur Web supplémentaires ou installer Manager Service. Reportez-vous à la section [Installer des composants de serveur Web IaaS supplémentaires](#) ou [Installer le service Active Manager Service](#).

Installer des composants de serveur Web IaaS supplémentaires

Le serveur Web donne accès à des fonctionnalités d'infrastructure dans vRealize Automation. Une fois le premier serveur Web installé, vous pouvez augmenter les performances en installant des serveurs Web IaaS supplémentaires.

N'installez pas Model Manager Data avec un composant de serveur Web supplémentaire. Seul le premier composant de serveur Web héberge Model Manager Data.

Conditions préalables

- [Installer un composant de site Web IaaS et Model Manager Data](#).
- Vérifiez que le nouveau serveur répond aux exigences dans la section [Serveurs Windows IaaS](#).
- Utilisez l'interface de gestion de dispositif vRealize Automation pour remplacer le certificat afin d'inclure le nom de domaine complet du nouveau nœud. Reportez-vous à *Remplacer les certificats dans le dispositif vRealize Automation* dans le guide de *Gestion de vRealize Automation*.
- Si vous avez installé déjà d'autres composants IaaS, vous devez connaître la phrase secrète de la base de données que vous avez créée.
- Si vous utilisez des équilibrages de charge dans votre environnement, vérifiez qu'ils correspondent aux exigences de configuration.

Procédure

- 1** Si vous utilisez un équilibrage de charge, désactivez les autres nœuds sous l'équilibrage de charge, puis vérifiez que le trafic est redirigé vers le nœud souhaité.

En outre, désactivez les contrôles de santé de l'équilibrage de charge jusqu'à ce que tous les composants vRealize Automation aient été installés et configurés.

- 2 Cliquez avec le bouton droit sur le fichier d'installation `setup__vrealize-automation-appliance-FQDN@5480.exe` et sélectionnez **Exécuter en tant qu'administrateur**.
- 3 Cliquez sur **Suivant**.
- 4 Acceptez le contrat de licence, puis cliquez sur **Suivant**.
- 5 Sur la page de connexion, fournissez les informations d'identification d'administrateur pour le dispositif vRealize Automation et vérifiez le certificat SSL.
 - a Entrez le nom d'utilisateur **root** et le mot de passe.

Le mot de passe est celui que vous avez spécifié lors du déploiement du dispositif vRealize Automation.
 - b Sélectionnez **Accepter le certificat**.
 - c Cliquez sur **Afficher le certificat**.

Comparez l'empreinte de certificat à l'empreinte définie pour le dispositif vRealize Automation. Vous pouvez afficher le certificat du dispositif vRealize Automation dans le navigateur du client si vous avez accédé à l'interface de gestion du dispositif vRealize Automation sur le port 5480.
- 6 Cliquez sur **Suivant**.
- 7 Sur la page Type d'installation, sélectionnez **Installation personnalisée**.
- 8 Dans la section Composant sur la page Type d'installation, sélectionnez **Serveur IaaS**.
- 9 Acceptez l'emplacement d'installation racine ou cliquez sur **Modifier** et sélectionnez le chemin d'installation.

Même dans un déploiement distribué, vous pouvez être amené à installer plusieurs composants IaaS sur un même serveur Windows.

Si vous installez plusieurs composants IaaS, veillez toujours à les installer au même endroit.
- 10 Cliquez sur **Suivant**.
- 11 Sélectionnez **Site Web** sur la page **Installation personnalisée du serveur IaaS**.
- 12 Sélectionnez un site Web parmi ceux qui sont disponibles ou acceptez le site Web par défaut dans l'onglet **Site Web Administration et Model Manager**.
- 13 Entrez un numéro de port disponible dans la zone de texte **Numéro de port** ou acceptez le port par défaut 443.
- 14 Cliquez sur **Tester la liaison** pour confirmer que le numéro de port est disponible.

15 Sélectionnez le certificat pour ce composant.

- a Si vous avez importé un certificat après avoir commencé l'installation, cliquez sur **Actualiser** pour mettre la liste à jour.
- b Sélectionnez le certificat à utiliser dans la section **Certificats disponibles**.
- c Si vous avez importé un certificat qui n'a pas de nom convivial et qui n'apparaît pas dans la liste, désélectionnez l'option **Afficher les certificats utilisant des noms conviviaux** et cliquez sur **Actualiser**.

Si vous effectuez l'installation dans un environnement qui n'utilise pas d'équilibrages de charge, vous pouvez sélectionner **Générer un certificat auto-signé** au lieu de sélectionner un certificat. Si vous installez des composants de site Web supplémentaires derrière un équilibrage de charge, ne générez pas de certificats auto-signés. Pour garantir que vous utilisez le même certificat sur tous les serveurs derrière l'équilibrage de charge, importez le certificat depuis le serveur Web IaaS principal.

- 16** (Facultatif) Cliquez sur **Afficher le certificat**, affichez le certificat et cliquez sur **OK** pour fermer la fenêtre d'information.
- 17** (Facultatif) Sélectionnez **Supprimer les incompatibilités de certificat** pour supprimer les erreurs de certificat. L'installation ignore les erreurs d'incompatibilité de nom de certificat et toutes les erreurs de correspondance de liste à distance de révocation de certificat.
Il s'agit d'une option moins sécurisée.
- 18** Dans la zone de texte **Serveur IaaS**, identifiez le premier composant de serveur Web IaaS.

Option	Description
Avec équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant de serveur Web IaaS, <i>web-load-balancer.mycompany.com:443</i> . N'entrez pas d'adresses IP.
Sans équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de la machine sur laquelle vous avez installé le premier composant de serveur Web IaaS, <i>web.mycompany.com:443</i> . N'entrez pas d'adresses IP.

Le port par défaut est 443.

- 19** Cliquez sur **Tester** pour vérifier la connexion du serveur.
- 20** Cliquez sur **Suivant**.

21 Terminez la vérification des conditions préalables.

Option	Description
Aucune erreur	Cliquez sur Suivant .
Erreurs non critiques	Cliquez sur Aucune correction .
Erreurs critiques	Si vous ne corrigez pas les erreurs critiques, l'installation échoue. Si des avertissements s'affichent, sélectionnez l'avertissement dans le volet gauche et suivez les instructions à droite. Résolvez toutes les erreurs critiques et cliquez sur Vérifier à nouveau pour vérifier.

22 Sur la page Paramètres de serveur et de compte, dans les zones de texte **Informations d'installation du serveur**, entrez le nom d'utilisateur et le mot de passe de l'utilisateur du compte de service ayant des privilèges administratifs sur le serveur d'installation actuel.

L'utilisateur du compte de service doit correspondre à un compte de domaine ayant des privilèges sur chaque serveur IaaS distribué. N'utilisez pas de comptes système locaux.

23 Fournissez la phrase secrète utilisée pour générer la clé de chiffrement qui protège la base de données.

Option	Description
Si vous avez déjà installé des composants dans cet environnement	Entrez la phrase secrète créée auparavant dans les zones de texte Phrase secrète et Confirmer .
S'il s'agit de la première installation	Entrez une phrase secrète dans les zones de texte Phrase secrète et Confirmer . Vous devez utiliser cette phrase secrète à chaque fois que vous installez un nouveau composant.

Conservez cette phrase secrète dans un lieu sûr pour l'utiliser ultérieurement.

24 Spécifiez le serveur de base de données IaaS, le nom de la base de données et la méthode d'authentification pour le serveur de base de données dans la zone de texte **Informations d'installation de la base de données Microsoft SQL**.

Il s'agit du serveur de base de données, du nom et des informations d'authentification que vous avez créés auparavant.

25 Cliquez sur **Suivant**.

26 Cliquez sur **Installer**.

27 Lorsque l'installation est terminée, désélectionnez **Me guider tout au long de la configuration initiale** et cliquez sur **Suivant**.

Étape suivante

[Installer le service Active Manager Service](#) .

Installer le service Active Manager Service

Le composant Manager Service actif est un service Windows qui coordonne la communication entre les instances de IaaS Distributed Execution Manager, la base de données, les agents, les agents proxy et SMTP.

À moins d'activer le basculement automatique de Manager Service, votre déploiement IaaS nécessite qu'une seule machine Windows exécute Manager Service de façon active à la fois. Le service doit être arrêté et configuré pour démarrer manuellement sur les machines de sauvegarde.

Reportez-vous à [À propos du basculement automatique de Manager Service](#).

Conditions préalables

- Si vous avez installé déjà d'autres composants IaaS, vous devez connaître la phrase secrète de la base de données que vous avez créée.
- (Facultatif) Si vous souhaitez installer Manager Service sur un autre site Web que le site Web par défaut, créez au préalable un site Web dans Internet Information Services.
- Vérifiez que vous disposez d'un certificat d'une autorité de certification importé dans IIS et que le certificat racine ou l'autorité de certification est approuvé(e). Tous les composants sous l'équilibrage de charge doivent avoir le même certificat.
- Vérifiez que l'équilibrage de charge du site Web est configuré et que la valeur du délai d'attente pour l'équilibrage de charge est définie sur 180 secondes au minimum.
- [Installer un composant de site Web IaaS et Model Manager Data.](#)

Procédure

- 1 Si vous utilisez un équilibrage de charge, désactivez les autres nœuds sous l'équilibrage de charge, puis vérifiez que le trafic est redirigé vers le nœud souhaité.

En outre, désactivez les contrôles de santé de l'équilibrage de charge jusqu'à ce que tous les composants vRealize Automation aient été installés et configurés.

- 2 Cliquez avec le bouton droit sur le fichier d'installation `setup__vrealize-automation-appliance-FQDN@5480.exe` et sélectionnez **Exécuter en tant qu'administrateur**.
- 3 Acceptez le contrat de licence, puis cliquez sur **Suivant**.

- 4 Sur la page de connexion, fournissez les informations d'identification d'administrateur pour le dispositif vRealize Automation et vérifiez le certificat SSL.

- a Entrez le nom d'utilisateur **root** et le mot de passe.

Le mot de passe est celui que vous avez spécifié lors du déploiement du dispositif vRealize Automation.

- b Sélectionnez **Accepter le certificat**.

- c Cliquez sur **Afficher le certificat**.

Comparez l'empreinte de certificat à l'empreinte définie pour le dispositif vRealize Automation. Vous pouvez afficher le certificat du dispositif vRealize Automation dans le navigateur du client si vous avez accédé à l'interface de gestion du dispositif vRealize Automation sur le port 5480.

- 5 Cliquez sur **Suivant**.

- 6 Sur la page Type d'installation, sélectionnez **Installation personnalisée**.

- 7 Dans la section Composant sur la page Type d'installation, sélectionnez **Serveur IaaS**.

- 8 Acceptez l'emplacement d'installation racine ou cliquez sur **Modifier** et sélectionnez le chemin d'installation.

Même dans un déploiement distribué, vous pouvez être amené à installer plusieurs composants IaaS sur un même serveur Windows.

Si vous installez plusieurs composants IaaS, veillez toujours à les installer au même endroit.

- 9 Cliquez sur **Suivant**.

- 10 Sélectionnez **Manager Service** sur la page **Installation personnalisée du serveur IaaS**.

- 11 Dans la zone de texte **Serveur IaaS**, identifiez le composant de serveur Web IaaS.

Option	Description
Avec équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant de serveur Web IaaS, <i>web-load-balancer.mycompany.com:443</i> . N'entrez pas d'adresses IP.
Sans équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de la machine sur laquelle vous avez installé le composant de serveur Web IaaS, <i>web.mycompany.com:443</i> . N'entrez pas d'adresses IP.

Le port par défaut est 443.

- 12 Sélectionnez **Nœud actif avec type de démarrage défini sur automatique**.

- 13 Sélectionnez un site Web parmi ceux qui sont disponibles ou acceptez le site Web par défaut dans l'onglet **Site Web Administration et Model Manager**.

- 14 Entrez un numéro de port disponible dans la zone de texte **Numéro de port** ou acceptez le port par défaut 443.
- 15 Cliquez sur **Tester la liaison** pour confirmer que le numéro de port est disponible.
- 16 Sélectionnez le certificat pour ce composant.
 - a Si vous avez importé un certificat après avoir commencé l'installation, cliquez sur **Actualiser** pour mettre la liste à jour.
 - b Sélectionnez le certificat à utiliser dans la section **Certificats disponibles**.
 - c Si vous avez importé un certificat qui n'a pas de nom convivial et qui n'apparaît pas dans la liste, désélectionnez l'option **Afficher les certificats utilisant des noms conviviaux** et cliquez sur **Actualiser**.

Si vous effectuez l'installation dans un environnement qui n'utilise pas d'équilibrages de charge, vous pouvez sélectionner **Générer un certificat auto-signé** au lieu de sélectionner un certificat. Si vous installez des composants de site Web supplémentaires derrière un équilibrage de charge, ne générez pas de certificats auto-signés. Pour garantir que vous utilisez le même certificat sur tous les serveurs derrière l'équilibrage de charge, importez le certificat depuis le serveur Web IaaS principal.

- 17 (Facultatif) Cliquez sur **Afficher le certificat**, affichez le certificat et cliquez sur **OK** pour fermer la fenêtre d'information.
- 18 Cliquez sur **Suivant**.
- 19 Vérifiez les conditions préalables et cliquez sur **Suivant**.
- 20 Sur la page Paramètres de serveur et de compte, dans les zones de texte **Informations d'installation du serveur**, entrez le nom d'utilisateur et le mot de passe de l'utilisateur du compte de service ayant des privilèges administratifs sur le serveur d'installation actuel.

L'utilisateur du compte de service doit correspondre à un compte de domaine ayant des privilèges sur chaque serveur IaaS distribué. N'utilisez pas de comptes système locaux.
- 21 Fournissez la phrase secrète utilisée pour générer la clé de chiffrement qui protège la base de données.

Option	Description
Si vous avez déjà installé des composants dans cet environnement	Entrez la phrase secrète créée auparavant dans les zones de texte Phrase secrète et Confirmer .
S'il s'agit de la première installation	Entrez une phrase secrète dans les zones de texte Phrase secrète et Confirmer . Vous devez utiliser cette phrase secrète à chaque fois que vous installez un nouveau composant.

Conservez cette phrase secrète dans un lieu sûr pour l'utiliser ultérieurement.

- 22** Spécifiez le serveur de base de données IaaS, le nom de la base de données et la méthode d'authentification pour le serveur de base de données dans la zone de texte **Informations d'installation de la base de données Microsoft SQL**.

Il s'agit du serveur de base de données, du nom et des informations d'authentification que vous avez créés auparavant.

- 23** Cliquez sur **Suivant**.

- 24** Cliquez sur **Installer**.

- 25** Lorsque l'installation est terminée, désélectionnez **Me guider tout au long de la configuration initiale** et cliquez sur **Suivant**.

- 26** Cliquez sur **Terminer**.

Étape suivante

- Pour garantir que l'instance de Manager Service que vous avez installée est l'instance active, vérifiez que le service vCloud Automation Center est en cours d'exécution et définissez-le sur le type de démarrage « Automatique ».
- Vous pouvez installer une instance supplémentaire du composant Manager Service en tant que sauvegarde passive que vous démarrez manuellement en cas de défaillance de l'instance active. Reportez-vous à [Installer un composant de sauvegarde Manager Service](#).
- Un administrateur système peut modifier la méthode d'authentification utilisée pour accéder à la base de données SQL lors de l'exécution (une fois l'installation terminée). Reportez-vous à [Configuration du service Windows pour accéder à la base de données IaaS](#).

Installer un composant de sauvegarde Manager Service

Le service de sauvegarde Manager Service assure la redondance et la haute disponibilité, et peut être démarré manuellement si le service actif s'arrête.

À moins d'activer le basculement automatique de Manager Service, votre déploiement IaaS nécessite qu'une seule machine Windows exécute Manager Service de façon active à la fois. Le service doit être arrêté et configuré pour démarrer manuellement sur les machines de sauvegarde.

Reportez-vous à [À propos du basculement automatique de Manager Service](#).

Conditions préalables

- Si vous avez installé déjà d'autres composants IaaS, vous devez connaître la phrase secrète de la base de données que vous avez créée.
- (Facultatif) Si vous souhaitez installer Manager Service sur un autre site Web que le site Web par défaut, créez au préalable un site Web dans Internet Information Services.

- Utilisez l'interface de gestion de dispositif vRealize Automation pour remplacer le certificat afin d'inclure le nom de domaine complet du nouveau nœud. Reportez-vous à *Remplacer les certificats dans le dispositif vRealize Automation* dans le guide de *Gestion de vRealize Automation*.
- Vérifiez que vous disposez d'un certificat d'une autorité de certification importé dans IIS et que le certificat racine ou l'autorité de certification est approuvé(e). Tous les composants sous l'équilibrage de charge doivent avoir le même certificat.
- Vérifiez que l'équilibrage de charge du site Web est configuré.
- [Installer un composant de site Web IaaS et Model Manager Data.](#)

Procédure

- 1 Si vous utilisez un équilibrage de charge, désactivez les autres nœuds sous l'équilibrage de charge, puis vérifiez que le trafic est redirigé vers le nœud souhaité.

En outre, désactivez les contrôles de santé de l'équilibrage de charge jusqu'à ce que tous les composants vRealize Automation aient été installés et configurés.
- 2 Cliquez avec le bouton droit sur le fichier d'installation `setup__vrealize-automation-appliance-FQDN@5480.exe` et sélectionnez **Exécuter en tant qu'administrateur**.
- 3 Cliquez sur **Suivant**.
- 4 Acceptez le contrat de licence, puis cliquez sur **Suivant**.
- 5 Sur la page de connexion, fournissez les informations d'identification d'administrateur pour le dispositif vRealize Automation et vérifiez le certificat SSL.
 - a Entrez le nom d'utilisateur **root** et le mot de passe.

Le mot de passe est celui que vous avez spécifié lors du déploiement du dispositif vRealize Automation.
 - b Sélectionnez **Accepter le certificat**.
 - c Cliquez sur **Afficher le certificat**.

Comparez l'empreinte de certificat à l'empreinte définie pour le dispositif vRealize Automation. Vous pouvez afficher le certificat du dispositif vRealize Automation dans le navigateur du client si vous avez accédé à l'interface de gestion du dispositif vRealize Automation sur le port 5480.
- 6 Cliquez sur **Suivant**.
- 7 Sur la page Type d'installation, sélectionnez **Installation personnalisée**.
- 8 Dans la section Composant sur la page Type d'installation, sélectionnez **Serveur IaaS**.
- 9 Acceptez l'emplacement d'installation racine ou cliquez sur **Modifier** et sélectionnez le chemin d'installation.

Même dans un déploiement distribué, vous pouvez être amené à installer plusieurs composants IaaS sur un même serveur Windows.

Si vous installez plusieurs composants IaaS, veuillez toujours à les installer au même endroit.

- 10 Cliquez sur **Suivant**.
- 11 Sélectionnez **Manager Service** sur la page **Installation personnalisée du serveur IaaS**.
- 12 Dans la zone de texte **Serveur IaaS**, identifiez le composant de serveur Web IaaS.

Option	Description
Avec équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant de serveur Web IaaS, <i>web-load-balancer.mycompany.com:443</i> . N'entrez pas d'adresses IP.
Sans équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de la machine sur laquelle vous avez installé le composant de serveur Web IaaS, <i>web.mycompany.com:443</i> . N'entrez pas d'adresses IP.

Le port par défaut est 443.

- 13 Sélectionnez **Nœud de reprise progressive après sinistre**
- 14 Sélectionnez un site Web parmi ceux qui sont disponibles ou acceptez le site Web par défaut dans l'onglet **Site Web Administration et Model Manager**.
- 15 Entrez un numéro de port disponible dans la zone de texte **Numéro de port** ou acceptez le port par défaut 443.
- 16 Cliquez sur **Tester la liaison** pour confirmer que le numéro de port est disponible.
- 17 Sélectionnez le certificat pour ce composant.
 - a Si vous avez importé un certificat après avoir commencé l'installation, cliquez sur **Actualiser** pour mettre la liste à jour.
 - b Sélectionnez le certificat à utiliser dans la section **Certificats disponibles**.
 - c Si vous avez importé un certificat qui n'a pas de nom convivial et qui n'apparaît pas dans la liste, désélectionnez l'option **Afficher les certificats utilisant des noms conviviaux** et cliquez sur **Actualiser**.

Si vous effectuez l'installation dans un environnement qui n'utilise pas d'équilibrages de charge, vous pouvez sélectionner **Générer un certificat auto-signé** au lieu de sélectionner un certificat. Si vous installez des composants de site Web supplémentaires derrière un équilibrage de charge, ne générez pas de certificats auto-signés. Pour garantir que vous utilisez le même certificat sur tous les serveurs derrière l'équilibrage de charge, importez le certificat depuis le serveur Web IaaS principal.

- 18 (Facultatif) Cliquez sur **Afficher le certificat**, affichez le certificat et cliquez sur **OK** pour fermer la fenêtre d'information.
- 19 Cliquez sur **Suivant**.
- 20 Vérifiez les conditions préalables et cliquez sur **Suivant**.

- 21** Sur la page Paramètres de serveur et de compte, dans les zones de texte **Informations d'installation du serveur**, entrez le nom d'utilisateur et le mot de passe de l'utilisateur du compte de service ayant des privilèges administratifs sur le serveur d'installation actuel.

L'utilisateur du compte de service doit correspondre à un compte de domaine ayant des privilèges sur chaque serveur IaaS distribué. N'utilisez pas de comptes système locaux.

- 22** Fournissez la phrase secrète utilisée pour générer la clé de chiffrement qui protège la base de données.

Option	Description
Si vous avez déjà installé des composants dans cet environnement	Entrez la phrase secrète créée auparavant dans les zones de texte Phrase secrète et Confirmer .
S'il s'agit de la première installation	Entrez une phrase secrète dans les zones de texte Phrase secrète et Confirmer . Vous devez utiliser cette phrase secrète à chaque fois que vous installez un nouveau composant.

Conservez cette phrase secrète dans un lieu sûr pour l'utiliser ultérieurement.

- 23** Spécifiez le serveur de base de données IaaS, le nom de la base de données et la méthode d'authentification pour le serveur de base de données dans la zone de texte **Informations d'installation de la base de données Microsoft SQL**.

Il s'agit du serveur de base de données, du nom et des informations d'authentification que vous avez créés auparavant.

- 24** Cliquez sur **Suivant**.

- 25** Cliquez sur **Installer**.

- 26** Lorsque l'installation est terminée, désélectionnez **Me guider tout au long de la configuration initiale** et cliquez sur **Suivant**.

- 27** Cliquez sur **Terminer**.

Étape suivante

- Pour garantir que l'instance de Manager Service que vous avez installée est une instance de sauvegarde passive, vérifiez que le service vRealize Automation n'est pas en cours d'exécution et définissez-le sur le type de démarrage « Manuel ».
- Un administrateur système peut modifier la méthode d'authentification utilisée pour accéder à la base de données SQL lors de l'exécution (une fois l'installation terminée). Reportez-vous à [Configuration du service Windows pour accéder à la base de données IaaS](#).

Installation des composants Distributed Execution Manager

Vous installez le DEM en tant que l'un des rôles : DEM Orchestrator ou DEM Worker. Vous devez installer au moins une instance de DEM pour chaque rôle et vous pouvez installer des instances de DEM supplémentaires pour prendre en charge le basculement et la haute disponibilité.

L'administrateur système doit choisir les machines d'installation répondant à la configuration système requise prédéfinie. DEM Orchestrator et DEM Worker peuvent se trouver sur une machine identique.

Au moment où vous prévoyez l'installation des DEM, tenez compte des considérations suivantes :

- Les instances DEM Orchestrator prennent en charge la haute disponibilité active-active. En règle générale, vous installez un DEM Orchestrator sur chaque machine Manager Service.
- Installez le DEM Orchestrator sur une machine disposant d'une forte connectivité réseau à l'hôte Model Manager.
- Installez un second DEM Orchestrator sur une machine différente pour le basculement.
- En règle générale, vous installez des DEM Workers sur le serveur IaaS Manager Service ou sur un serveur distinct. Le serveur doit disposer d'une connectivité réseau à l'hôte Model Manager.
- Vous pouvez installer des instances de DEM supplémentaires pour la redondance et l'évolutivité, notamment plusieurs instances sur la même machine.

L'installation du DEM nécessite une configuration spécifique en fonction des points de terminaison que vous utilisez. Reportez-vous à [Hôte DEM \(Distributed Execution Manager\) IaaS](#).

Installer les instances Distributed Execution Manager

Vous devez installer au moins une instance de DEM Worker et une instance de DEM Orchestrator. La procédure d'installation est la même pour les deux rôles.

Les instances DEM Orchestrator prennent en charge la haute disponibilité active-active. Généralement, vous installez une instance DEM Orchestrator unique sur chaque machine Manager Service. Vous pouvez installer les instances DEM Orchestrator et DEM Worker sur la même machine.

Conditions préalables

[Télécharger le programme d'installation de vRealize Automation IaaS](#).

Procédure

- 1 Cliquez avec le bouton droit sur le fichier d'installation `setup__vrealize-automation-appliance-FQDN@5480.exe` et sélectionnez **Exécuter en tant qu'administrateur**.
- 2 Cliquez sur **Suivant**.
- 3 Acceptez le contrat de licence, puis cliquez sur **Suivant**.

- 4 Sur la page de connexion, fournissez les informations d'identification d'administrateur pour le dispositif vRealize Automation et vérifiez le certificat SSL.

- a Entrez le nom d'utilisateur **root** et le mot de passe.

Le mot de passe est celui que vous avez spécifié lors du déploiement du dispositif vRealize Automation.

- b Sélectionnez **Accepter le certificat**.

- c Cliquez sur **Afficher le certificat**.

Comparez l'empreinte de certificat à l'empreinte définie pour le dispositif vRealize Automation. Vous pouvez afficher le certificat du dispositif vRealize Automation dans le navigateur du client si vous avez accédé à l'interface de gestion du dispositif vRealize Automation sur le port 5480.

- 5 Cliquez sur **Suivant**.

- 6 Sur la page Type d'installation, sélectionnez **Installation personnalisée**.

- 7 Sur la page Type d'installation, sous Sélection du composant, sélectionnez **Distributed Execution Managers**.

- 8 Acceptez l'emplacement d'installation racine ou cliquez sur **Modifier** et sélectionnez le chemin d'installation.

Même dans un déploiement distribué, vous pouvez être amené à installer plusieurs composants IaaS sur un même serveur Windows.

Si vous installez plusieurs composants IaaS, veillez toujours à les installer au même endroit.

- 9 Cliquez sur **Suivant**.

- 10 Vérifiez les conditions préalables et cliquez sur **Suivant**.

- 11 Entrez les informations d'identification de connexion avec lesquelles le service sera exécuté.

Le compte de service doit avoir des privilèges d'administrateur local et être le compte de domaine que vous utilisiez lors de l'installation d'IaaS. Le compte de service a des privilèges sur chaque serveur IaaS distribué et ne doit pas être un compte système local.

- 12 Cliquez sur **Suivant**.

- 13 Sélectionnez le type d'installation dans le menu déroulant **Rôle DEM**.

Option	Description
Travailleur	Le travailleur exécute les workflows.
Orchestrator	L'orchestrator supervise les activités du travailleur, y compris la planification et le traitement préalable des workflows, et contrôle le statut en ligne du DEM Worker.

14 Entrez un nom unique identifiant ce DEM dans la zone de texte **Nom du DEM**.

Le nom ne doit pas inclure d'espaces et ne doit pas comporter plus de 128 caractères. Si vous entrez un nom qui a été utilisé auparavant, le message suivant s'affiche : « Un DEM portant le même nom existe déjà. Pour entrer un autre nom pour ce DEM, cliquez sur Oui. Si vous restaurez ou réinstallez un DEM avec le même nom, cliquez sur Non. »

15 (Facultatif) Entrez une description de cette instance dans **Description du DEM****16** Entrez les noms d'hôte et les ports dans les zones de texte **Nom d'hôte Manager Service** et **Nom d'hôte Model Manager Web Service**.

Option	Description
Avec équilibrage de charge	Entrez le nom de domaine complet et le numéro de port des équilibres de charge pour le composant Manager Service et le serveur Web qui héberge Model Manager, <i>mgr-svc-load-balancer.mycompany.com:443</i> et <i>web-load-balancer.mycompany.com:443</i> . N'entrez pas d'adresses IP.
Sans équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de la machine sur laquelle vous avez installé le composant Manager Service et le serveur Web qui héberge Model Manager, <i>mgr-svc.mycompany.com:443</i> et <i>web.mycompany.com:443</i> . N'entrez pas d'adresses IP.

Le port par défaut est 443.

17 (Facultatif) Cliquez sur **Tester** pour tester les connexions aux services Manager Service et Model Manager Web Service.**18** Cliquez sur **Ajouter**.**19** Cliquez sur **Suivant**.**20** Cliquez sur **Installer**.**21** Lorsque l'installation est terminée, désélectionnez **Me guider tout au long de la configuration initiale** et cliquez sur **Suivant**.**22** Cliquez sur **Terminer**.**Étape suivante**

- Vérifiez que le service est en cours d'exécution et que le journal ne présente aucune erreur. Le nom du service est VMware DEM *Role - Name*, où le rôle est Orchestrator ou Travailleur. L'emplacement du journal est *Install Location\Distributed Execution Manager\Name\Logs*.
- Répétez cette procédure pour installer des instances DEM supplémentaires.

Configurer DEM pour se connecter à SCVMM sur un chemin d'installation différent

Par défaut, le fichier de configuration de DEM Worker utilise le chemin d'installation par défaut de la console de Microsoft System Center Virtual Machine Manager (SCVMM). Si vous installez la

console SCVMM dans un emplacement autre que celui par défaut, vous devez mettre à jour le fichier.

Vous avez besoin de cette procédure uniquement si vous avez des points de terminaison et des agents SCVMM.

Conditions préalables

- Souvenez-vous du chemin d'accès par défaut dans lequel vous avez installé la console SCVMM.

Le chemin suivant est le chemin par défaut que vous devez remplacer dans le fichier de configuration.

```
path="{ProgramFiles}\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"
```

Procédure

- 1 Arrêtez le service DEM Worker.
- 2 Ouvrez le fichier suivant dans un éditeur de texte.
Program Files (x86)\VMware\VCAC\Distributed Execution Manager*instance-name*\DynamicOps.DEM.exe.config
- 3 Localisez la section <assemblyLoadConfiguration>.
- 4 Mettez à jour chaque chemin, en utilisant l'exemple suivant comme guide.

```
<assemblyLoadConfiguration>
  <assemblies>
    <!-- List of required assemblies for Scvmm -->
    <add name="Errors" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
    <add name="Microsoft.SystemCenter.VirtualMachineManager" path="D:\Microsoft System Center 2012
R2\Virtual Machine Manager\bin"/>
    <add name="Remoting" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
    <add name="TraceWrapper" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager
\bin"/>
    <add name="Utils" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
  </assemblies>
</assemblyLoadConfiguration>
```

- 5 Enregistrez et fermez DynamicOps.DEM.exe.config.
- 6 Redémarrez le service DEM Worker.

Résultats

Pour plus d'informations, reportez-vous à [DEM Workers avec SCVMM](#).

Vous trouverez des informations supplémentaires sur la préparation de l'environnement SCVMM et la création d'un point de terminaison SCVMM dans *Configuration de vRealize Automation*.

Configuration du service Windows pour accéder à la base de données laaS

Un administrateur système peut modifier la méthode d'authentification utilisée pour accéder à la base de données SQL lors de l'exécution (une fois l'installation terminée). Par défaut, l'identité Windows du compte actuellement connecté est utilisée pour connecter la base de données une fois son installation terminée.

Activez l'accès à la base de données laaS pour l'utilisateur du service

Si la base de données SQL est installée sur un hôte distinct du Manager Service, l'accès à la base de données depuis Manager Service doit être activé. Si le nom d'utilisateur avec lequel Manager Service doit s'exécuter est défini comme propriétaire de la base de données, aucune action n'est requise. Si l'utilisateur n'est pas le propriétaire de la base de données, l'administrateur système doit lui accorder l'accès.

Conditions préalables

- Choisir un scénario de base de données laaS.
- Vérifiez que le nom d'utilisateur avec lequel Manager Service doit s'exécuter est défini comme propriétaire de la base de données.

Procédure

- 1 Accédez au sous-répertoire Base de données situé dans le répertoire où vous avez extrait le fichier d'installation compressé (zip).
- 2 Extrayez l'archive DBInstall.zip dans un répertoire local.
- 3 Connectez-vous à l'hôte de la base de données en tant qu'utilisateur avec le rôle **sysadmin** dans l'instance SQL Server.
- 4 Modifiez VMPSOpsUser.sql et remplacez toutes les instances de \$(Service User) par l'utilisateur (à l'étape 3) avec lequel Manager Service doit s'exécuter.

Ne remplacez pas ServiceUser dans la ligne se terminant par WHERE name = N'ServiceUser').
- 5 Ouvrez SQL Server Management Studio.
- 6 Sélectionnez la base de données (vCAC par défaut) dans **Bases de données** dans le volet gauche.
- 7 Cliquez sur **Nouvelle requête**.

La fenêtre Requête SQL s'ouvre dans le volet droit.
- 8 Collez tout le contenu modifié de VMPSOpsUser.sql dans la fenêtre de la requête.
- 9 Cliquez sur **Exécuter**.

Résultats

L'accès à la base de données est activé depuis Manager Service.

Configurer le compte des services Windows pour utiliser l'authentification SQL

Par défaut, le compte des services Windows accède à la base de données lors de l'exécution, même si vous avez configuré la base de données pour l'authentification SQL. Vous pouvez modifier l'authentification au moment de l'exécution de l'authentification Windows à l'authentification SQL.

Il convient notamment de modifier l'authentification au moment de l'exécution lorsque la base de données se trouve dans un domaine non approuvé.

Conditions préalables

Vérifiez que la base de données SQL Server de vRealize Automation existe. Commencez avec [Choisir un scénario de base de données laaS](#).

Procédure

- 1 En utilisant un compte disposant de privilèges d'administrateur, connectez-vous au serveur Windows laaS qui héberge le composant Manager Service.
- 2 Dans **Outils d'administration > Services**, arrêtez le service **VMware vCloud Automation Center**.
- 3 Ouvrez les fichiers suivants dans un éditeur de texte.

```
C:\Program Files (x86)\VMware\VCAC\Server\ManagerService.exe.config
C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Web\Web.config
```

- 4 Dans chaque fichier, localisez la section <connectionStrings>.

- 5 Remplacez

```
Integrated Security=True;
```

par

```
User Id=database-username;Password=database-password;
```

- 6 Enregistrez et fermez les fichiers.

```
ManagerService.exe.config
Web.config
```

- 7 Démarrez le service **VMware vCloud Automation Center**.
- 8 Utilisez la commande `iisreset` pour redémarrer IIS.

Vérifier les services laaS

Après l'installation, l'administrateur système vérifie que les services laaS sont en cours d'exécution. Si c'est bien le cas, l'installation est réussie.

Procédure

- 1 Sur le poste de travail Windows de la machine IaaS, sélectionnez **Outils d'administration > Services**.
- 2 Recherchez les services suivants et vérifiez que leur état est Démarré et que le type de démarrage est défini sur Automatique.
 - VMware DEM – Orchestrator – *Name* où *Name* est la chaîne fournie dans la zone **Nom du DEM** pendant l'installation.
 - VMware DEM – Worker – *Name* où *Name* est la chaîne fournie dans la zone **Nom du DEM** pendant l'installation.
 - Agent VMware vCloud Automation Center *Agent name*
 - Service VMware vCloud Automation Center
- 3 Fermez la fenêtre **Services**.

Installation d'agents vRealize Automation

vRealize Automation utilise des agents pour s'intégrer à des systèmes externes. Un administrateur système peut sélectionner des agents à installer pour communiquer avec d'autres plates-formes de virtualisation.

vRealize Automation utilise les types d'agents suivants pour gérer des systèmes externes :

- Agents proxy de l'hyperviseur (serveurs vSphere, Citrix Xen Server et Microsoft Hyper-V Server)
- Agents d'intégration de l'EPI (External Provisioning Infrastructure)
- Agents VDI (Virtual Desktop Infrastructure)
- Agents WMI (Windows Management Instrumentation)

Pour la haute disponibilité, vous pouvez installer plusieurs agents pour un seul point de terminaison. Installez chaque agent redondant sur un serveur distinct, mais nommez et configurez-les de manière identique. Les agents redondants fournissent une certaine tolérance aux pannes, mais pas de basculement. Par exemple, si vous installez deux agents vSphere, l'un sur le serveur A et l'autre sur le serveur B, et que le serveur A devient indisponible, l'agent installé sur le serveur B continue de traiter les éléments de travail. En revanche, l'agent du serveur B est dans l'impossibilité de terminer le traitement d'un élément de travail que l'agent du serveur A a déjà démarré.

Vous avez la possibilité d'installer un agent vSphere dans le cadre de votre installation minimale, mais une fois celle-ci terminée, vous pouvez également ajouter d'autres agents, y compris un agent vSphere supplémentaire. Dans un déploiement distribué, vous installez tous vos agents après avoir terminé l'installation distribuée de base. Les agents que vous installez dépendent des ressources de votre infrastructure.

Pour plus d'informations sur l'utilisation des agents vSphere, reportez-vous à la section [Conditions requises de l'agent vSphere](#).

Définir la stratégie d'exécution PowerShell sur RemoteSigned

Vous devez définir la stratégie d'exécution de PowerShell de Restricted à RemoteSigned ou Unrestricted pour permettre aux scripts PowerShell locaux de s'exécuter.

Pour en savoir plus sur la stratégie d'exécution de PowerShell, consultez l'[Article Microsoft PowerShell sur les stratégies d'exécution](#). Si votre stratégie d'exécution PowerShell est gérée au niveau de la stratégie de groupe, contactez votre service d'assistance informatique à propos de ses restrictions sur les modifications de stratégie, et consultez l'[Article Microsoft PowerShell sur les paramètres de stratégie de groupe](#).

Conditions préalables

- Vérifiez que Microsoft PowerShell est installé sur l'hôte d'installation avant l'installation de l'agent. La version requise dépend du système d'exploitation sur l'hôte d'installation. Reportez-vous à l'aide et à l'assistance Windows.
- Pour plus d'informations sur la stratégie d'exécution PowerShell, exécutez `help about_signing` ou `help Set-ExecutionPolicy` sur l'invite de commande PowerShell.

Procédure

- 1 En utilisant un compte d'administrateur, connectez-vous à la machine hôte IaaS sur laquelle l'agent est installé.
- 2 Sélectionnez **Démarrer > Tous les programmes > Version Windows PowerShell > Windows PowerShell**.
- 3 Pour RemoteSigned, exécutez `Set-ExecutionPolicy RemoteSigned`.
- 4 Pour Unrestricted, exécutez `Set-ExecutionPolicy Unrestricted`.
- 5 Vérifiez que la commande n'a pas entraîné d'erreur.
- 6 Tapez **Exit** à l'invite de commande PowerShell.

Choisir le scénario d'installation de l'agent

Les agents que vous devez installer dépendent des systèmes externes avec lesquels vous souhaitez les intégrer.

Tableau 5-10. Choisir un scénario d'installation

Scénario d'intégration	Conditions requises et procédures pour l'agent
Provisionner des machines cloud via l'intégration avec un environnement cloud tel que Amazon Web Services ou Red Hat Enterprise Linux OpenStack Platform.	Il n'est pas nécessaire d'installer un agent.
Provisionner des machines virtuelles via l'intégration avec un environnement vSphere.	Installation et configuration de l'agent Proxy pour vSphere

Tableau 5-10. Choisir un scénario d'installation (suite)

Scénario d'intégration	Conditions requises et procédures pour l'agent
Provisionner des machines virtuelles via l'intégration avec un environnement Microsoft Hyper-V Server.	Installation de l'agent Proxy pour Hyper-V ou XenServer
Provisionner des machines virtuelles via l'intégration avec un environnement XenServer.	<ul style="list-style-type: none"> ■ Installation de l'agent Proxy pour Hyper-V ou XenServer ■ Installation de l'agent EPI pour Citrix
Provisionner des machines virtuelles via l'intégration avec un environnement XenDesktop.	<ul style="list-style-type: none"> ■ Installation de l'agent VDI pour XenDesktop ■ Installation de l'agent EPI pour Citrix
Exécutez des scripts Visual Basic en tant qu'étapes supplémentaires dans le processus de provisionnement avant ou après de provisionner une machine, ou lors de l'annulation du provisionnement.	Installation de l'agent EPI pour les scripts Visual Basic
Collecter des données à partir des machines Windows provisionnées, par exemple le statut Active Directory ou le propriétaire d'une machine.	Installation de l'agent WMI pour les demandes WMI à distance
Provisionner des machines virtuelles via l'intégration avec toute autre plate-forme virtuelle prise en charge.	Il n'est pas nécessaire d'installer un agent.

Emplacement et conditions d'installation de l'agent

Un administrateur système installe généralement les agents sur le serveur vRealize Automation qui héberge le composant Manager Service actif.

Si un agent est installé sur un autre hôte, la configuration réseau doit permettre la communication entre l'agent la machine d'installation de Manager Services.

Chaque agent est installé sous un nom unique dans son propre répertoire, `Agents\agentname`, sous le répertoire d'installation de vRealize Automation (généralement `Program Files(x86)\VMware\vCAC`), avec sa configuration stockée dans le fichier `VRMAgent.exe.config` dans ce répertoire.

Installation et configuration de l'agent Proxy pour vSphere

Un administrateur système installe des agents proxy pour communiquer avec des instances du serveur vSphere. Les agents découvrent le travail disponible, récupèrent les informations de l'hôte et font des rapports sur les éléments de travail terminés et autres modifications de l'état de l'hôte.

Conditions requises de l'agent vSphere

Les informations d'identification du point de terminaison vSphere ou les informations d'identification avec lesquelles l'agent s'exécute doivent avoir un accès administratif à l'hôte d'installation. Plusieurs agents vSphere doivent respecter les conditions requises de configuration de vRealize Automation.

Informations d'identification

Lors de la création d'un point de terminaison représentant l'instance de vCenter Server à faire gérer par un agent vSphere, celui-ci peut utiliser les informations d'identification avec lesquelles le service s'exécute pour interagir avec vCenter Server ou spécifier des informations d'identification de point de terminaison distinctes.

Le privilège VApp.Import permet de déployer une machine vSphere en utilisant les paramètres importés à partir d'un fichier OVF. Les détails sur ce privilège vSphere sont disponibles dans la [Documentation de vSphere SDK](#). Si vous prévoyez d'utiliser un point de terminaison vSphere pour déployer des machines virtuelles à partir de modèles OVF, vérifiez que vos informations d'identification incluent le privilège vSphere VApp.Import dans l'instance de vCenter Server associée au point de terminaison.

Le tableau suivant répertorie les autorisations dont les informations d'identification du point de terminaison vSphere doivent disposer pour gérer une instance de vCenter Server. Ces autorisations doivent être activées pour tous les clusters de vCenter Server et pas uniquement les clusters qui hébergeront des points de terminaison.

Tableau 5-11. Autorisations requises pour que l'agent vSphere gère une instance de vCenter Server

Valeur de l'attribut		Autorisation
Banque de données		Allouer l'espace
		Parcourir la BD
Cluster de banques de données		Configurer un cluster de banques de données
Dossier		Créer l'annuaire
		Supprimer le dossier
Global		Gérer les attributs personnalisés
		Définir un attribut personnalisé
Réseau		Assigner réseau
Autorisations		Modifier autorisation
vApp		Importer
		Configuration de l'application vApp
Ressource		Attribuer une machine virtuelle au pool de ressources
		Migrer la machine virtuelle hors tension
		Migrer la machine virtuelle sous tension
Machine virtuelle	Inventaire	Créer à partir d'un modèle existant
		Créer nouveau
		Déplacer

Tableau 5-11. Autorisations requises pour que l'agent vSphere gère une instance de vCenter Server (suite)

Valeur de l'attribut	Autorisation
Interaction	Supprimer
	Configurer les supports CD
	Interaction de console
	Connexion de périphérique
	Mettre hors tension
	Mettre sous tension
	Réinitialiser
	Interrompre
	Installation d'outils
Configuration	Ajouter un disque existant
	Ajouter un nouveau disque
	Ajouter ou supprimer un périphérique
	Supprimer un disque
	Avancé
	Changer le nombre de CPU
	Changer la ressource
	Développer un disque virtuel
	Suivi des changements de disques
	Mémoire
	Modifier les paramètres de périphérique
	Renommer
	Définir une annotation (version 5.0 et ultérieure)
	Paramètres
	Emplacement du fichier d'échange
Provisionnement	Personnaliser
	Modèle de clone
	Cloner machine virtuelle
	Déployer modèle

Tableau 5-11. Autorisations requises pour que l'agent vSphere gère une instance de vCenter Server (suite)

Valeur de l'attribut	Autorisation
	Lire les spécifications de personnalisation
État	Créer un snapshot
	Supprimer le snapshot
	Restaurer le snapshot

Désactivez ou reconfigurez les logiciels tiers susceptibles de modifier l'état de l'alimentation des machines virtuelles situées à l'extérieur de vRealize Automation. Ces modifications peuvent interférer avec la gestion du cycle de vie de la machine par vRealize Automation.

Installer l'agent vSphere

Installez un agent vSphere pour gérer les instances vCenter Server. Pour la haute disponibilité, vous pouvez installer un second agent vSphere redondant pour la même instance vCenter Server. Vous devez nommer et configurer les deux agents vSphere de manière identique, et les installer sur des machines différentes.

Conditions préalables

- Installez IaaS, y compris le serveur Web et l'hôte Manager Service.
- Vérifiez que la machine sur laquelle vous installez l'agent se trouve sur un domaine approuvé par le domaine où les composants IaaS sont installés.
- Vérifiez que la configuration requise dans [Conditions requises de l'agent vSphere](#) est respectée.
- Si vous avez déjà créé un point de terminaison vSphere qui sera utilisé avec cet agent, notez son nom.
- [Télécharger le programme d'installation de vRealize AutomationIaaS.](#)

Procédure

- 1 Cliquez avec le bouton droit sur le fichier d'installation `setup__vrealize-automation-appliance-FQDN@5480.exe` et sélectionnez **Exécuter en tant qu'administrateur**.
- 2 Cliquez sur **Suivant**.
- 3 Acceptez le contrat de licence, puis cliquez sur **Suivant**.

- 4 Sur la page de connexion, fournissez les informations d'identification d'administrateur pour le dispositif vRealize Automation et vérifiez le certificat SSL.

- a Entrez le nom d'utilisateur **root** et le mot de passe.

Le mot de passe est celui que vous avez spécifié lors du déploiement du dispositif vRealize Automation.

- b Sélectionnez **Accepter le certificat**.

- c Cliquez sur **Afficher le certificat**.

Comparez l'empreinte de certificat à l'empreinte définie pour le dispositif vRealize Automation. Vous pouvez afficher le certificat du dispositif vRealize Automation dans le navigateur du client si vous avez accédé à l'interface de gestion du dispositif vRealize Automation sur le port 5480.

- 5 Sur la page Type d'installation, sélectionnez **Installation personnalisée**.

- 6 Dans la zone Sélection du composant, sélectionnez **Agents proxy**.

- 7 Acceptez l'emplacement d'installation racine ou cliquez sur **Modifier** et sélectionnez le chemin d'installation.

Même dans un déploiement distribué, vous pouvez être amené à installer plusieurs composants IaaS sur un même serveur Windows.

Si vous installez plusieurs composants IaaS, veillez toujours à les installer au même endroit.

- 8 Cliquez sur **Suivant**.

- 9 Connectez-vous avec des privilèges d'administrateur pour les services Windows sur la machine d'installation.

Le service doit être exécuté sur la même machine d'installation.

- 10 Cliquez sur **Suivant**.

- 11 Sélectionnez vSphere dans la liste **Type d'agent**.

- 12 Entrez un identifiant pour cet agent dans la zone de texte **Nom de l'agent**.

Conservez le nom de l'agent, les informations d'identification, le nom du point de terminaison et l'instance de plate-forme pour chaque agent. Vous aurez besoin de ces informations pour configurer les points de terminaison et pour ajouter des hôtes par la suite.

Important Pour la haute disponibilité, vous pouvez ajouter des agents redondants et les configurer de manière identique. Sinon, conservez les agents uniques.

Option	Description
Agent redondant	Installez les agents redondants sur des serveurs distincts. Nommez et configurez les agents redondants de manière identique.
Agent autonome	Attribuez un nom unique à l'agent.

13 Configurez une connexion à l'hôte d'IaaS Manager Service.

Option	Description
Avec équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant Manager Service, <i>mgr-svc-load-balancer.mycompany.com:443</i> . N'entrez pas d'adresses IP.
Sans équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de la machine sur laquelle vous avez installé le composant Manager Service, <i>mgr-svc.mycompany.com:443</i> . N'entrez pas d'adresses IP.

Le port par défaut est 443.

14 Configurez une connexion au serveur Web IaaS.

Option	Description
Avec équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant de serveur Web, <i>web-load-balancer.mycompany.com:443</i> . N'entrez pas d'adresses IP.
Sans équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de la machine sur laquelle vous avez installé le composant de serveur Web, <i>web.mycompany.com:443</i> . N'entrez pas d'adresses IP.

Le port par défaut est 443.

15 Cliquez sur **Tester** pour vérifier la connectivité avec chaque hôte.**16** Entrez le nom du point de terminaison.

Pour que le point de terminaison fonctionne, le nom que vous configurez dans vRealize Automation doit correspondre au nom du point de terminaison fourni à l'agent proxy vSphere lors de l'installation.

17 Cliquez sur **Ajouter**.**18** Cliquez sur **Suivant**.**19** Cliquez sur **Installer** pour lancer l'installation.

Au bout de quelques minutes, un message de réussite s'affiche.

20 Cliquez sur **Suivant**.**21** Cliquez sur **Terminer**.**22** Vérifiez si l'installation a été effectuée correctement.**23** (Facultatif) Ajoutez plusieurs agents avec des configurations différentes et un point de terminaison sur le même système.

Étape suivante

[Configurer l'agent vSphere.](#)

Configurer l'agent vSphere

Configurez l'agent vSphere en préparation à la création et à l'utilisation de points de terminaison vSphere dans des Blueprints vRealize Automation.

Vous employez l'utilitaire de l'agent proxy pour modifier des parties chiffrées du fichier de configuration de l'agent ou pour modifier la stratégie de suppression de machines pour les plates-formes de virtualisation. Seule une partie du fichier de configuration de l'agent `VRMAgent.exe.config` est chiffrée. Par exemple, la section `serviceConfiguration` n'est pas chiffrée.

Conditions préalables

En utilisant un compte avec privilèges d'administrateur, connectez-vous au serveur IaaS Windows sur lequel vous avez installé l'agent vSphere.

Procédure

- 1 Ouvrez une invite de commandes Windows en tant qu'administrateur.
- 2 Passez au dossier d'installation de l'agent, où *agent-name* est le dossier contenant l'agent vSphere.

```
cd %SystemDrive%\Program Files (x86)\VMware\VCAC\Agents\agent-name
```

- 3 (Facultatif) Pour afficher les paramètres de configuration actuels, entrez la commande suivante.

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config get
```

Voici un exemple de sortie de la commande.

```
managementEndpointName: VCEndpoint
doDeletes: True
```

- 4 (Facultatif) Pour modifier le nom du point de terminaison que vous avez configuré lors de l'installation, utilisez la commande suivante.

```
set managementEndpointName
```

Par exemple : `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set managementEndpointName my-endpoint`

Vous utilisez ce processus pour renommer le point de terminaison dans vRealize Automation plutôt que de modifier les points de terminaison.

- 5 (Facultatif) Pour configurer la stratégie de suppression de machines virtuelles, utilisez la commande suivante.

```
set doDeletes
```

Par exemple : `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set doDeletes false`

Option	Description
true	(Par défaut) Supprimer les machines virtuelles détruites dans vRealize Automation depuis vCenter Server.
false	Déplacez les machines virtuelles détruites dans vRealize Automation vers le répertoire VRMDelated dans vCenter Server.

- Ouvrez **Outils d'administration > Services** et redémarrez le service vRealize Automation Agent – *agent-name*.

Étape suivante

Pour la haute disponibilité, vous pouvez installer et configurer un agent redondant pour votre point de terminaison. Installez chaque agent redondant sur un serveur distinct, mais nommez et configurez les agents de manière identique.

Installation de l'agent Proxy pour Hyper-V ou XenServer

Un administrateur système installe des agents proxy pour communiquer avec des instances du serveur Hyper-V ou XenServer. Les agents découvrent le travail disponible, récupèrent les informations de l'hôte et font des rapports sur les éléments de travail terminés et autres modifications de l'état de l'hôte.

Conditions requises pour Hyper-V et XenServer

Les agents proxy Hyper-V Hypervisor requièrent des informations d'identification pour l'installation.

Les informations d'identification avec lesquelles l'agent de service est exécuté doivent disposer d'un accès d'administration à l'hôte d'installation.

Des informations d'identification de niveau administrateur sont requises pour toutes les instances XenServer ou Hyper-V sur les hôtes qui doivent être gérés par l'agent.

Si vous utilisez des pools Xen, tous les nœuds qu'ils contiennent doivent être identifiés par leurs noms de domaines complets.

Note Par défaut, Hyper-V n'est pas configuré pour la gestion à distance. Un agent proxy vRealize AutomationHyper-V ne peut pas communiquer avec un serveur Hyper-V si la gestion à distance n'a pas été activée.

Pour obtenir des informations sur la procédure de configuration de Hyper-V pour la gestion à distance, reportez-vous à la documentation Microsoft Windows Server.

Installer l'agent Hyper-V ou XenServer

L'agent Hyper-V gère les instances de serveur Hyper-V. L'agent XenServer gère les instances de serveur XenServer.

Conditions préalables

- Installez IaaS, y compris le serveur Web et l'hôte Manager Service.
- [Télécharger le programme d'installation de vRealize AutomationIaaS](#).
- Vérifiez que les agents proxy de l'hyperviseur Hyper-V ont les mêmes informations d'identification d'administrateur système.
- Vérifiez que les informations d'identification avec lesquelles le service d'agent est exécuté ont des droits d'accès d'administration à l'hôte d'installation.
- Vérifiez que toutes les instances XenServer ou Hyper-V sur les hôtes qui doivent être gérés par l'agent ont des informations d'identification du niveau administrateur.
- Si vous utilisez des pools Xen, notez que tous les nœuds au sein du pool Xen doivent être identifiés par leurs noms de domaine complets.

vRealize Automation ne peut pas gérer ni communiquer avec les nœuds qui ne sont pas identifiés par leur nom de domaine complet au sein du pool Xen.

- Configurez Hyper-V pour la gestion à distance afin de permettre la communication du serveur Hyper-V avec les agents proxy vRealize AutomationHyper-V.

Pour obtenir des informations sur la procédure de configuration de Hyper-V pour la gestion à distance, reportez-vous à la documentation Microsoft Windows Server.

Procédure

- 1 Cliquez avec le bouton droit sur le fichier d'installation `setup__vrealize-automation-appliance-FQDN@5480.exe` et sélectionnez **Exécuter en tant qu'administrateur**.
- 2 Cliquez sur **Suivant**.
- 3 Acceptez le contrat de licence, puis cliquez sur **Suivant**.
- 4 Sur la page de connexion, fournissez les informations d'identification d'administrateur pour le dispositif vRealize Automation et vérifiez le certificat SSL.
 - a Entrez le nom d'utilisateur **root** et le mot de passe.
Le mot de passe est celui que vous avez spécifié lors du déploiement du dispositif vRealize Automation.
 - b Sélectionnez **Accepter le certificat**.
 - c Cliquez sur **Afficher le certificat**.
Comparez l'empreinte de certificat à l'empreinte définie pour le dispositif vRealize Automation. Vous pouvez afficher le certificat du dispositif vRealize Automation dans le navigateur du client si vous avez accédé à l'interface de gestion du dispositif vRealize Automation sur le port 5480.
- 5 Sur la page Type d'installation, sélectionnez **Installation personnalisée**.
- 6 Sélectionnez **Sélection du composant** sur la page Type d'installation.

- 7 Acceptez l'emplacement d'installation racine ou cliquez sur **Modifier** et sélectionnez le chemin d'installation.

Même dans un déploiement distribué, vous pouvez être amené à installer plusieurs composants IaaS sur un même serveur Windows.

Si vous installez plusieurs composants IaaS, veillez toujours à les installer au même endroit.

- 8 Cliquez sur **Suivant**.

- 9 Connectez-vous avec des privilèges d'administrateur pour les services Windows sur la machine d'installation.

Le service doit être exécuté sur la même machine d'installation.

- 10 Cliquez sur **Suivant**.

- 11 Sélectionnez l'agent dans la liste **Type d'agent**.

- Xen
- Hyper-V

- 12 Entrez un identifiant pour cet agent dans la zone de texte **Nom de l'agent**.

Conservez le nom de l'agent, les informations d'identification, le nom du point de terminaison et l'instance de plate-forme pour chaque agent. Vous aurez besoin de ces informations pour configurer les points de terminaison et pour ajouter des hôtes par la suite.

Important Pour la haute disponibilité, vous pouvez ajouter des agents redondants et les configurer de manière identique. Sinon, conservez les agents uniques.

Option	Description
Agent redondant	Installez les agents redondants sur des serveurs distincts. Nommez et configurez les agents redondants de manière identique.
Agent autonome	Attribuez un nom unique à l'agent.

- 13 Communiquez le **Nom de l'agent** à l'administrateur IaaS qui configure les points de terminaison.

Pour permettre l'accès et la collecte des données, le point de terminaison doit être lié à l'agent qui a été configuré pour lui.

14 Configurez une connexion à l'hôte d'IaaS Manager Service.

Option	Description
Avec équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant Manager Service, <i>mgr-svc-load-balancer.mycompany.com:443</i> . N'entrez pas d'adresses IP.
Sans équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de la machine sur laquelle vous avez installé le composant Manager Service, <i>mgr-svc.mycompany.com:443</i> . N'entrez pas d'adresses IP.

Le port par défaut est 443.

15 Configurez une connexion au serveur Web IaaS.

Option	Description
Avec équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant de serveur Web, <i>web-load-balancer.mycompany.com:443</i> . N'entrez pas d'adresses IP.
Sans équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de la machine sur laquelle vous avez installé le composant de serveur Web, <i>web.mycompany.com:443</i> . N'entrez pas d'adresses IP.

Le port par défaut est 443.

16 Cliquez sur **Tester** pour vérifier la connectivité avec chaque hôte.**17** Entrez les informations d'identification d'un utilisateur avec des autorisations de niveau administrateur sur l'instance de serveur géré.**18** Cliquez sur **Ajouter**.**19** Cliquez sur **Suivant**.**20** (Facultatif) Ajoutez un autre agent.

Par exemple, vous pouvez ajouter un agent Xen si vous avez précédemment ajouté l'agent Hyper-V.

21 Cliquez sur **Installer** pour lancer l'installation.

Au bout de quelques minutes, un message de réussite s'affiche.

22 Cliquez sur **Suivant**.**23** Cliquez sur **Terminer**.**24** Vérifiez si l'installation a été effectuée correctement.

Étape suivante

Pour la haute disponibilité, vous pouvez installer et configurer un agent redondant pour votre point de terminaison. Installez chaque agent redondant sur un serveur distinct, mais nommez et configurez les agents de manière identique.

[Configurer l'agent Hyper-V ou XenServer.](#)

Configurer l'agent Hyper-V ou XenServer

Un administrateur système peut modifier les paramètres de configuration de l'agent proxy, par exemple la stratégie de suppression des plates-formes de virtualisation. Vous pouvez utiliser l'utilitaire de l'agent proxy pour modifier les configurations initiales qui sont chiffrées dans le fichier de configuration de l'agent.

Conditions préalables

Connectez-vous en tant qu'**administrateur système** à la machine sur laquelle vous avez installé l'agent.

Procédure

- 1 Passez au répertoire d'installation des agents, où *agent_name* est le répertoire qui contient l'agent proxy et qui est également le nom sous lequel l'agent est installé.

```
cd Program Files (x86)\VMware\VCAC Agents\agent_name
```

- 2 Afficher les paramètres de configuration actuels.

```
Entrez DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config get
```

Voici un exemple de sortie de commande :

```
Username: XSadmin
```

- 3 Entrez la commande set pour modifier une propriété, où *propriété* est l'une des options affichée dans le tableau.

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set la valeur de la propriété
```

Si vous omettez la *valeur*, l'utilitaire vous invite à renseigner une nouvelle valeur.

Propriété	Description
username	Le nom d'utilisateur représentant les informations d'identification de niveau administrateur pour le serveur XenServer ou Hyper-V avec lequel l'agent communique.
password	Le mot de passe pour le nom d'utilisateur de niveau administrateur.

- 4 Cliquez sur **Démarrer > Outils d'administration > Services**, puis redémarrez le service vRealize Automation Agent – *nom de l'agent*.

Exemple : Modifier les informations d'identification de niveau administrateur

Entrez la commande suivante pour modifier les informations d'identification de niveau administrateur pour la plate-forme de virtualisation spécifiée lors de l'installation de l'agent.

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set username jsmith
```

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set password
```

Étape suivante

Pour la haute disponibilité, vous pouvez installer et configurer un agent redondant pour votre point de terminaison. Installez chaque agent redondant sur un serveur distinct, mais nommez et configurez les agents de manière identique.

Installation de l'agent VDI pour XenDesktop

vRealize Automation utilise des agents VDI PowerShell pour enregistrer les machines XenDesktop qu'il provisionne auprès de systèmes de gestion de bureau externes.

L'agent d'intégration VDI fournit aux propriétaires de machines enregistrées une connexion directe à l'interface Web XenDesktop. Vous pouvez installer un agent en tant qu'agent dédié à l'interaction avec un seul DDC (Desktop Delivery Controller) ou en tant qu'agent général pouvant interagir avec plusieurs DDC.

Conditions requises de XenDesktop

Un administrateur système installe un agent VDI pour intégrer des serveurs XenDesktop à vRealize Automation.

Vous pouvez installer un agent VDI général pour interagir avec plusieurs serveurs. Si vous installez un agent dédié par serveur pour l'équilibrage de charge ou des motifs d'autorisation, vous devez fournir le nom du serveur DDC XenDesktop lors de l'installation de l'agent. Un agent dédié peut gérer uniquement les demandes d'enregistrement adressées au serveur spécifiées dans sa configuration.

Pour plus d'informations sur les versions prises en charge de XenDesktop pour les serveurs DDC XenDesktop, reportez-vous à la *Matrice de prise en charge de vRealize Automation* sur le site Web de VMware.

Hôte et informations d'identification d'installation

Les informations d'identification avec lesquelles l'agent s'exécute doivent disposer d'un accès administratif à tous les serveurs DDC XenDesktop avec lesquels il interagit.

Conditions requises de XenDesktop

Le nom attribué à l'hôte XenServer sur votre serveur XenDesktop doit correspondre à l'UUID du pool de serveurs Xen dans XenCenter. Consultez [Définir le nom d'hôte XenServer](#) pour plus d'informations.

Chaque serveur DDC XenDesktop auprès duquel vous comptez enregistrer des machines doit être configuré comme suit :

- Le type du groupe/catalogue doit être défini sur **Existant** pour être utilisé avec vRealize Automation.
- Le nom d'un hôte vCenter Server sur un serveur DDC doit correspondre au nom de l'instance de vCenter Server entré dans le point de terminaison vSphere vRealize Automation, sans le domaine. Le point de terminaison doit être configuré avec un nom de domaine complet et non avec une adresse IP. Par exemple, si l'adresse dans le point de terminaison est `https://virtual-center27.domain/sdk`, le nom de l'hôte sur le serveur DDC doit être défini sur `virtual-center27`.

Si votre point de terminaison vSphere vRealize Automation a été configuré avec une adresse IP, vous devez le modifier pour utiliser un nom de domaine complet. Pour plus d'informations sur la configuration des points de terminaison, reportez-vous à la documentation *Configuration d'IaaS*.

Conditions requises de l'hôte de l'agent XenDesktop

Citrix XenDesktop SDK doit être installé. Le SDK pour XenDesktop est inclus dans le disque d'installation de XenDesktop.

Vérifiez que Microsoft PowerShell est installé sur l'hôte d'installation avant l'installation de l'agent. La version requise dépend du système d'exploitation sur l'hôte d'installation. Reportez-vous à l'aide et à l'assistance Windows.

La stratégie d'exécution MS PowerShell est définie sur RemoteSigned ou Unrestricted. Reportez-vous à [Définir la stratégie d'exécution PowerShell sur RemoteSigned](#).

Pour plus d'informations sur la stratégie d'exécution PowerShell, exécutez `help about_signing` ou `help Set-ExecutionPolicy` sur l'invite de commande PowerShell.

Définir le nom d'hôte XenServer

Dans XenDesktop, le nom attribué à l'hôte XenServer sur votre serveur XenDesktop doit correspondre à l'UUID du pool de serveurs Xen dans XenCenter. Si aucun XenPool n'est configuré, le nom doit correspondre à l'UUID de l'hôte XenServer lui-même.

Procédure

- 1 Dans Citrix XenCenter, sélectionnez votre XenPool ou XenServer autonome et cliquez sur l'onglet **Général**. Enregistrez l'UUID.
- 2 Lorsque vous ajoutez votre pool de serveurs XenServer ou votre hôte autonome à XenDesktop, tapez l'UUID enregistré à l'étape précédente en tant que nom de la **Connexion**.

Installer l'agent XenDesktop

Les agents PowerShell d'intégration de bureau virtuel (VDI) s'intègrent au système de bureaux virtuels externe, comme XenDesktop et Citrix. Utilisez un agent PowerShell VDI pour gérer la machine XenDesktop.

Conditions préalables

- Installez IaaS, y compris le serveur Web et l'hôte Manager Service.
- Vérifiez que la configuration requise dans [Conditions requises de XenDesktop](#) est respectée.
- [Télécharger le programme d'installation de vRealize Automation IaaS](#).

Procédure

- 1 Cliquez avec le bouton droit sur le fichier d'installation `setup__vrealize-automation-appliance-FQDN@5480.exe` et sélectionnez **Exécuter en tant qu'administrateur**.
- 2 Cliquez sur **Suivant**.
- 3 Acceptez le contrat de licence, puis cliquez sur **Suivant**.
- 4 Sur la page de connexion, fournissez les informations d'identification d'administrateur pour le dispositif vRealize Automation et vérifiez le certificat SSL.
 - a Entrez le nom d'utilisateur **root** et le mot de passe.

Le mot de passe est celui que vous avez spécifié lors du déploiement du dispositif vRealize Automation.
 - b Sélectionnez **Accepter le certificat**.
 - c Cliquez sur **Afficher le certificat**.

Comparez l'empreinte de certificat à l'empreinte définie pour le dispositif vRealize Automation. Vous pouvez afficher le certificat du dispositif vRealize Automation dans le navigateur du client si vous avez accédé à l'interface de gestion du dispositif vRealize Automation sur le port 5480.
- 5 Cliquez sur **Suivant**.
- 6 Sur la page Type d'installation, sélectionnez **Installation personnalisée**.
- 7 Sélectionnez **Agents proxy** dans le volet Sélection du composant.
- 8 Acceptez l'emplacement d'installation racine ou cliquez sur **Modifier** et sélectionnez le chemin d'installation.

Même dans un déploiement distribué, vous pouvez être amené à installer plusieurs composants IaaS sur un même serveur Windows.

Si vous installez plusieurs composants IaaS, veuillez toujours à les installer au même endroit.
- 9 Cliquez sur **Suivant**.
- 10 Connectez-vous avec des privilèges d'administrateur pour les services Windows sur la machine d'installation.

Le service doit être exécuté sur la même machine d'installation.
- 11 Cliquez sur **Suivant**.
- 12 Sélectionnez **PowerShell VDI** dans la liste **Type d'agent**.

13 Entrez un identifiant pour cet agent dans la zone de texte **Nom de l'agent**.

Conservez le nom de l'agent, les informations d'identification, le nom du point de terminaison et l'instance de plate-forme pour chaque agent. Vous aurez besoin de ces informations pour configurer les points de terminaison et pour ajouter des hôtes par la suite.

Important Pour la haute disponibilité, vous pouvez ajouter des agents redondants et les configurer de manière identique. Sinon, conservez les agents uniques.

Option	Description
Agent redondant	Installez les agents redondants sur des serveurs distincts. Nommez et configurez les agents redondants de manière identique.
Agent autonome	Attribuez un nom unique à l'agent.

14 Configurez une connexion à l'hôte d'IaaS Manager Service.

Option	Description
Avec équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant Manager Service, <i>mgr-svc-load-balancer.mycompany.com:443</i> . N'entrez pas d'adresses IP.
Sans équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de la machine sur laquelle vous avez installé le composant Manager Service, <i>mgr-svc.mycompany.com:443</i> . N'entrez pas d'adresses IP.

Le port par défaut est 443.

15 Configurez une connexion au serveur Web IaaS.

Option	Description
Avec équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant de serveur Web, <i>web-load-balancer.mycompany.com:443</i> . N'entrez pas d'adresses IP.
Sans équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de la machine sur laquelle vous avez installé le composant de serveur Web, <i>web.mycompany.com:443</i> . N'entrez pas d'adresses IP.

Le port par défaut est 443.

16 Cliquez sur **Tester** pour vérifier la connectivité avec chaque hôte.**17** Sélectionnez la **Version de VDI**.**18** Entrez le nom de domaine complet du serveur géré dans la zone de texte **Serveur VDI**.**19** Cliquez sur **Ajouter**.

20 Cliquez sur **Suivant**.

21 Cliquez sur **Installer** pour lancer l'installation.

Au bout de quelques minutes, un message de réussite s'affiche.

22 Cliquez sur **Suivant**.

23 Cliquez sur **Terminer**.

24 Vérifiez si l'installation a été effectuée correctement.

25 (Facultatif) Ajoutez plusieurs agents avec des configurations différentes et un point de terminaison sur le même système.

Étape suivante

Pour la haute disponibilité, vous pouvez installer et configurer un agent redondant pour votre point de terminaison. Installez chaque agent redondant sur un serveur distinct, mais nommez et configurez les agents de manière identique.

Installation de l'agent EPI pour Citrix

Les agents EPI PowerShell intègrent des machines externes Citrix au processus de provisionnement. L'agent EPI diffuse à la demande les images du disque Citrix à partir desquelles les machines démarrent et s'exécutent.

L'agent EPI dédié interagit avec un serveur de provisionnement externe unique. Vous devez installer un agent EPI pour chaque instance du serveur de provisionnement Citrix.

Conditions requises pour Citrix Provisioning Server

Un administrateur système utilise des agents External Provisioning Infrastructure (EPI) pour intégrer les serveurs de provisionnement Citrix et pour activer l'utilisation des scripts Visual Basic dans le processus de provisionnement.

Emplacement d'installation et informations d'identification

Installez l'agent sur l'hôte PVS pour les instances de Citrix Provisioning Services. Vérifiez que l'hôte d'installation répond aux [Conditions requises pour l'agent hôte Citrix](#) avant d'installer l'agent.

Même si un agent EPI peut généralement interagir avec plusieurs serveurs, Citrix Provisioning Server requiert un agent EPI dédié. Vous devez installer un agent EPI pour chaque instance de Citrix Provisioning Server, en fournissant le nom du serveur qui l'héberge. Les informations d'identification avec lesquelles l'agent s'exécute doivent avoir un accès administratif à l'instance de Citrix Provisioning Server.

Reportez-vous à *Matrice de prise en charge de vRealize Automation* pour plus d'informations sur les versions de Citrix PVS prises en charge.

Conditions requises pour l'agent hôte Citrix

PowerShell et Citrix Provisioning Services SDK doivent être installés sur l'hôte d'installation avant d'installer l'agent. Pour plus de détails, reportez-vous à *Matrice de prise en charge de vRealize Automation* sur le site Web de VMware.

Vérifiez que Microsoft PowerShell est installé sur l'hôte d'installation avant l'installation de l'agent. La version requise dépend du système d'exploitation sur l'hôte d'installation. Reportez-vous à l'aide et à l'assistance Windows.

Vous devez également vous assurer que le composant logiciel enfichable de PowerShell est installé. Pour plus d'informations, reportez-vous au *Guide du programmeur PowerShell pour Citrix Provisioning Services* sur le site Web de Citrix.

La stratégie d'exécution MS PowerShell est définie sur RemoteSigned ou Unrestricted. Reportez-vous à [Définir la stratégie d'exécution PowerShell sur RemoteSigned](#).

Pour plus d'informations sur la stratégie d'exécution PowerShell, exécutez `help about_signing` ou `help Set-ExecutionPolicy` sur l'invite de commande PowerShell.

Installer l'agent Citrix

Les agents PowerShell d'intégration de provisionnement externe (EPI) intègrent des systèmes externes dans le processus de provisionnement des machines. Utilisez l'agent PowerShell EPI pour l'intégration à un serveur Citrix pour permettre le provisionnement de machines par diffusion à la demande de disque.

Conditions préalables

- Installez IaaS, y compris le serveur Web et l'hôte Manager Service.
- Vérifiez que la configuration requise dans [Conditions requises pour Citrix Provisioning Server](#) est respectée.
- [Télécharger le programme d'installation de vRealize AutomationIaaS](#).

Procédure

- 1 Cliquez avec le bouton droit sur le fichier d'installation `setup__vrealize-automation-appliance-FQDN@5480.exe` et sélectionnez **Exécuter en tant qu'administrateur**.
- 2 Cliquez sur **Suivant**.
- 3 Acceptez le contrat de licence, puis cliquez sur **Suivant**.

- 4 Sur la page de connexion, fournissez les informations d'identification d'administrateur pour le dispositif vRealize Automation et vérifiez le certificat SSL.

- a Entrez le nom d'utilisateur **root** et le mot de passe.

Le mot de passe est celui que vous avez spécifié lors du déploiement du dispositif vRealize Automation.

- b Sélectionnez **Accepter le certificat**.

- c Cliquez sur **Afficher le certificat**.

Comparez l'empreinte de certificat à l'empreinte définie pour le dispositif vRealize Automation. Vous pouvez afficher le certificat du dispositif vRealize Automation dans le navigateur du client si vous avez accédé à l'interface de gestion du dispositif vRealize Automation sur le port 5480.

- 5 Sur la page Type d'installation, sélectionnez **Installation personnalisée**.

- 6 Sélectionnez **Sélection du composant** sur la page Type d'installation.

- 7 Acceptez l'emplacement d'installation racine ou cliquez sur **Modifier** et sélectionnez le chemin d'installation.

Même dans un déploiement distribué, vous pouvez être amené à installer plusieurs composants IaaS sur un même serveur Windows.

Si vous installez plusieurs composants IaaS, veillez toujours à les installer au même endroit.

- 8 Cliquez sur **Suivant**.

- 9 Connectez-vous avec des privilèges d'administrateur pour les services Windows sur la machine d'installation.

Le service doit être exécuté sur la même machine d'installation.

- 10 Cliquez sur **Suivant**.

- 11 Dans la liste Type d'agent, sélectionnez **Power Shell EPI**.

- 12 Entrez un identifiant pour cet agent dans la zone de texte **Nom de l'agent**.

Conservez le nom de l'agent, les informations d'identification, le nom du point de terminaison et l'instance de plate-forme pour chaque agent. Vous aurez besoin de ces informations pour configurer les points de terminaison et pour ajouter des hôtes par la suite.

Important Pour la haute disponibilité, vous pouvez ajouter des agents redondants et les configurer de manière identique. Sinon, conservez les agents uniques.

Option	Description
Agent redondant	Installez les agents redondants sur des serveurs distincts. Nommez et configurez les agents redondants de manière identique.
Agent autonome	Attribuez un nom unique à l'agent.

13 Configurez une connexion à l'hôte d'IaaS Manager Service.

Option	Description
Avec équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant Manager Service, <i>mgr-svc-load-balancer.mycompany.com:443</i> . N'entrez pas d'adresses IP.
Sans équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de la machine sur laquelle vous avez installé le composant Manager Service, <i>mgr-svc.mycompany.com:443</i> . N'entrez pas d'adresses IP.

Le port par défaut est 443.

14 Configurez une connexion au serveur Web IaaS.

Option	Description
Avec équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant de serveur Web, <i>web-load-balancer.mycompany.com:443</i> . N'entrez pas d'adresses IP.
Sans équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de la machine sur laquelle vous avez installé le composant de serveur Web, <i>web.mycompany.com:443</i> . N'entrez pas d'adresses IP.

Le port par défaut est 443.

15 Cliquez sur **Tester** pour vérifier la connectivité avec chaque hôte.**16** Sélectionnez le type d'EPI.**17** Entrez le nom de domaine complet du serveur géré dans la zone de texte **Serveur EPI**.**18** Cliquez sur **Ajouter**.**19** Cliquez sur **Suivant**.**20** Cliquez sur **Installer** pour lancer l'installation.

Au bout de quelques minutes, un message de réussite s'affiche.

21 Cliquez sur **Suivant**.**22** Cliquez sur **Terminer**.**23** Vérifiez si l'installation a été effectuée correctement.**24** (Facultatif) Ajoutez plusieurs agents avec des configurations différentes et un point de terminaison sur le même système.

Étape suivante

Pour la haute disponibilité, vous pouvez installer et configurer un agent redondant pour votre point de terminaison. Installez chaque agent redondant sur un serveur distinct, mais nommez et configurez les agents de manière identique.

Installation de l'agent EPI pour les scripts Visual Basic

Un administrateur système peut définir des scripts Visual Basic comme étapes supplémentaires du processus de provisionnement avant ou après le provisionnement d'une machine ou lors de l'annulation du provisionnement d'une machine. Avant d'exécuter des scripts Visual Basic, vous devez installer un EPI PowerShell.

Les scripts Visual Basic sont spécifiés dans le Blueprint à partir duquel les machines sont provisionnées. Ces scripts ont accès à toutes les propriétés personnalisées associées à la machine et peuvent mettre à jour leurs valeurs. L'étape suivante du workflow a ensuite accès à ces nouvelles valeurs.

Vous pouvez, par exemple, utiliser un script pour générer des certificats ou des jetons de sécurité avant le provisionnement afin de les utiliser lors du provisionnement des machines.

Pour autoriser les scripts pendant le provisionnement, vous devez installer un type spécifique d'agent EPI et placer les scripts que vous souhaitez utiliser sur le système sur lequel l'agent est installé.

Lors de l'exécution d'un script, l'agent EPI transmet toutes les propriétés personnalisées de la machine comme arguments au script. Pour renvoyer des valeurs de propriétés mises à jour, vous devez placer ces propriétés dans un dictionnaire et appeler une fonction vRealize Automation. Un exemple de script est inclus dans le sous-répertoire des scripts du répertoire d'installation de l'agent EPI. Ce script contient un en-tête permettant de charger tous les arguments dans un dictionnaire, un corps dans lequel vous pouvez inclure votre ou vos fonctions et un pied de page permettant de renvoyer les valeurs de propriétés personnalisées mises à jour.

Note Vous pouvez installer plusieurs agents EPI/VBScripts sur plusieurs serveurs et effectuer le provisionnement avec un agent spécifique et les scripts Visual Basic de l'hôte de cet agent. Si vous avez besoin d'effectuer cette opération, contactez le support client de VMware.

Conditions requises pour les scripts Visual Basic

Un administrateur système installe des agents EPI pour permettre l'utilisation de scripts Visual Basic au cours du processus de provisionnement.

Le tableau suivant présente les conditions requises s'appliquant pour l'installation d'un agent EPI permettant d'activer l'utilisation de scripts Visual Basic dans le processus de provisionnement.

Tableau 5-12. Agents EPI pour l'écriture de scripts Visual

Conditions requises	Description
Informations d'identification	Les informations d'identification avec lesquelles l'agent s'exécute doit avoir un accès administratif à l'hôte d'installation.
Microsoft PowerShell	Microsoft PowerShell doit être installé sur l'hôte d'installation avant l'installation de l'agent : la version requise dépend du système d'exploitation de l'hôte d'installation et peut avoir été installée avec ce système d'exploitation. Pour plus d'informations, consultez la page http://support.microsoft.com .
Stratégie d'exécution MS PowerShell	<p>La stratégie d'exécution de MS PowerShell doit être définie sur RemoteSigned ou Unrestricted.</p> <p>Pour plus d'informations sur la stratégie d'exécution de PowerShell, exécutez l'une des commandes suivantes à l'invite de commande PowerShell :</p> <pre>help about_signing help Set-ExecutionPolicy</pre>

Installer l'agent pour les scripts Visual Basic

Les agents Power Shell d'intégration de provisionnement externe (EPI) permettent d'intégrer des systèmes externes dans le processus de provisionnement des machines. Utilisez un agent EPI pour exécuter les scripts Visual Basic comme étapes supplémentaires lors du processus de provisionnement.

Conditions préalables

- Installez IaaS, y compris le serveur Web et l'hôte Manager Service.
- Vérifiez que la configuration requise dans [Conditions requises pour les scripts Visual Basic](#) est respectée.
- [Télécharger le programme d'installation de vRealize AutomationIaaS](#).

Procédure

- 1 Cliquez avec le bouton droit sur le fichier d'installation `setup__vrealize-automation-appliance-FQDN@5480.exe` et sélectionnez **Exécuter en tant qu'administrateur**.
- 2 Cliquez sur **Suivant**.
- 3 Acceptez le contrat de licence, puis cliquez sur **Suivant**.

- 4 Sur la page de connexion, fournissez les informations d'identification d'administrateur pour le dispositif vRealize Automation et vérifiez le certificat SSL.

- a Entrez le nom d'utilisateur **root** et le mot de passe.

Le mot de passe est celui que vous avez spécifié lors du déploiement du dispositif vRealize Automation.

- b Sélectionnez **Accepter le certificat**.

- c Cliquez sur **Afficher le certificat**.

Comparez l'empreinte de certificat à l'empreinte définie pour le dispositif vRealize Automation. Vous pouvez afficher le certificat du dispositif vRealize Automation dans le navigateur du client si vous avez accédé à l'interface de gestion du dispositif vRealize Automation sur le port 5480.

- 5 Sur la page Type d'installation, sélectionnez **Installation personnalisée**.

- 6 Sélectionnez **Sélection du composant** sur la page Type d'installation.

- 7 Acceptez l'emplacement d'installation racine ou cliquez sur **Modifier** et sélectionnez le chemin d'installation.

Même dans un déploiement distribué, vous pouvez être amené à installer plusieurs composants IaaS sur un même serveur Windows.

Si vous installez plusieurs composants IaaS, veillez toujours à les installer au même endroit.

- 8 Cliquez sur **Suivant**.

- 9 Connectez-vous avec des privilèges d'administrateur pour les services Windows sur la machine d'installation.

Le service doit être exécuté sur la même machine d'installation.

- 10 Cliquez sur **Suivant**.

- 11 Dans la liste Type d'agent, sélectionnez **Power Shell EPI**.

- 12 Entrez un identifiant pour cet agent dans la zone de texte **Nom de l'agent**.

Conservez le nom de l'agent, les informations d'identification, le nom du point de terminaison et l'instance de plate-forme pour chaque agent. Vous aurez besoin de ces informations pour configurer les points de terminaison et pour ajouter des hôtes par la suite.

Important Pour la haute disponibilité, vous pouvez ajouter des agents redondants et les configurer de manière identique. Sinon, conservez les agents uniques.

Option	Description
Agent redondant	Installez les agents redondants sur des serveurs distincts. Nommez et configurez les agents redondants de manière identique.
Agent autonome	Attribuez un nom unique à l'agent.

13 Configurez une connexion à l'hôte d'IaaS Manager Service.

Option	Description
Avec équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant Manager Service, <i>mgr-svc-load-balancer.mycompany.com:443</i> . N'entrez pas d'adresses IP.
Sans équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de la machine sur laquelle vous avez installé le composant Manager Service, <i>mgr-svc.mycompany.com:443</i> . N'entrez pas d'adresses IP.

Le port par défaut est 443.

14 Configurez une connexion au serveur Web IaaS.

Option	Description
Avec équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant de serveur Web, <i>web-load-balancer.mycompany.com:443</i> . N'entrez pas d'adresses IP.
Sans équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de la machine sur laquelle vous avez installé le composant de serveur Web, <i>web.mycompany.com:443</i> . N'entrez pas d'adresses IP.

Le port par défaut est 443.

15 Cliquez sur **Tester** pour vérifier la connectivité avec chaque hôte.**16** Sélectionnez le type d'EPI.**17** Entrez le nom de domaine complet du serveur géré dans la zone de texte **Serveur EPI**.**18** Cliquez sur **Ajouter**.**19** Cliquez sur **Suivant**.**20** Cliquez sur **Installer** pour lancer l'installation.

Au bout de quelques minutes, un message de réussite s'affiche.

21 Cliquez sur **Suivant**.**22** Cliquez sur **Terminer**.**23** Vérifiez si l'installation a été effectuée correctement.**24** (Facultatif) Ajoutez plusieurs agents avec des configurations différentes et un point de terminaison sur le même système.

Installation de l'agent WMI pour les demandes WMI à distance

Un administrateur système active le protocole WMI et installe l'agent WMI sur toutes les machines Windows gérées pour autoriser la gestion des données et des opérations. L'agent doit collecter des données auprès des machines Windows, comme l'état Active Directory du propriétaire d'une machine.

Activer les demandes WMI à distance sur les machines Windows

Pour utiliser les agents WMI, les demandes WMI à distance doivent être activées sur les serveurs Windows gérés.

Procédure

- 1 Dans chaque domaine contenant des machines virtuelles provisionnées et gérées, créez un groupe Active Directory et ajoutez-le aux informations d'identification du service des agents WMI qui exécutent les demandes WMI à distance sur les machines provisionnées.
- 2 Activez les demandes WMI à distance pour les groupes Active Directory contenant les informations d'identification d'agent sur chaque machine provisionnée Windows.

Installer l'agent WMI

L'agent Windows Management Instrumentation (WMI) permet la collecte des données à partir des machines gérées Windows.

Conditions préalables

- Installez IaaS, y compris le serveur Web et l'hôte Manager Service.
- Vérifiez que la configuration requise dans [Activer les demandes WMI à distance sur les machines Windows](#) est respectée.
- [Télécharger le programme d'installation de vRealize AutomationIaaS](#).

Procédure

- 1 Cliquez avec le bouton droit sur le fichier d'installation `setup__vrealize-automation-appliance-FQDN@5480.exe` et sélectionnez **Exécuter en tant qu'administrateur**.
- 2 Cliquez sur **Suivant**.
- 3 Acceptez le contrat de licence, puis cliquez sur **Suivant**.

- 4 Sur la page de connexion, fournissez les informations d'identification d'administrateur pour le dispositif vRealize Automation et vérifiez le certificat SSL.

- a Entrez le nom d'utilisateur **root** et le mot de passe.

Le mot de passe est celui que vous avez spécifié lors du déploiement du dispositif vRealize Automation.

- b Sélectionnez **Accepter le certificat**.

- c Cliquez sur **Afficher le certificat**.

Comparez l'empreinte de certificat à l'empreinte définie pour le dispositif vRealize Automation. Vous pouvez afficher le certificat du dispositif vRealize Automation dans le navigateur du client si vous avez accédé à l'interface de gestion du dispositif vRealize Automation sur le port 5480.

- 5 Sur la page Type d'installation, sélectionnez **Installation personnalisée**.

- 6 Sélectionnez **Sélection du composant** sur la page Type d'installation.

- 7 Acceptez l'emplacement d'installation racine ou cliquez sur **Modifier** et sélectionnez le chemin d'installation.

Même dans un déploiement distribué, vous pouvez être amené à installer plusieurs composants IaaS sur un même serveur Windows.

Si vous installez plusieurs composants IaaS, veillez toujours à les installer au même endroit.

- 8 Cliquez sur **Suivant**.

- 9 Connectez-vous avec des privilèges d'administrateur pour les services Windows sur la machine d'installation.

Le service doit être exécuté sur la même machine d'installation.

- 10 Cliquez sur **Suivant**.

- 11 Sélectionnez **WMI** dans la liste **Type d'agent**.

- 12 Entrez un identifiant pour cet agent dans la zone de texte **Nom de l'agent**.

Conservez le nom de l'agent, les informations d'identification, le nom du point de terminaison et l'instance de plate-forme pour chaque agent. Vous aurez besoin de ces informations pour configurer les points de terminaison et pour ajouter des hôtes par la suite.

Important Pour la haute disponibilité, vous pouvez ajouter des agents redondants et les configurer de manière identique. Sinon, conservez les agents uniques.

Option	Description
Agent redondant	Installez les agents redondants sur des serveurs distincts. Nommez et configurez les agents redondants de manière identique.
Agent autonome	Attribuez un nom unique à l'agent.

13 Configurez une connexion à l'hôte d'IaaS Manager Service.

Option	Description
Avec équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant Manager Service, <i>mgr-svc-load-balancer.mycompany.com:443</i> . N'entrez pas d'adresses IP.
Sans équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de la machine sur laquelle vous avez installé le composant Manager Service, <i>mgr-svc.mycompany.com:443</i> . N'entrez pas d'adresses IP.

Le port par défaut est 443.

14 Configurez une connexion au serveur Web IaaS.

Option	Description
Avec équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant de serveur Web, <i>web-load-balancer.mycompany.com:443</i> . N'entrez pas d'adresses IP.
Sans équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de la machine sur laquelle vous avez installé le composant de serveur Web, <i>web.mycompany.com:443</i> . N'entrez pas d'adresses IP.

Le port par défaut est 443.

15 Cliquez sur **Tester** pour vérifier la connectivité avec chaque hôte.**16** Cliquez sur **Ajouter**.**17** Cliquez sur **Suivant**.**18** Cliquez sur **Installer** pour lancer l'installation.

Au bout de quelques minutes, un message de réussite s'affiche.

19 Cliquez sur **Suivant**.**20** Cliquez sur **Terminer**.**21** Vérifiez si l'installation a été effectuée correctement.**22** (Facultatif) Ajoutez plusieurs agents avec des configurations différentes et un point de terminaison sur le même système.

Installation silencieuse de vRealize Automation

6

vRealize Automation inclut des options pour l'installation silencieuse basée sur un script à partir de la ligne de commande et l'installation silencieuse basée sur API. Les deux approches imposent que vous prépariez d'avance les valeurs que vous devriez normalement saisir manuellement lors d'une installation classique.

Ce chapitre contient les rubriques suivantes :

- [À propos de l'installation silencieuse de vRealize Automation](#)
- [Effectuer une installation silencieuse de vRealize Automation](#)
- [Effectuer une installation silencieuse de l'agent de gestion de vRealize Automation](#)
- [Fichier de réponses pour installation silencieuse de vRealize Automation](#)
- [La ligne de commande d'installation de vRealize Automation](#)
- [API d'installation de vRealize Automation](#)
- [Convertir entre propriétés silencieuses vRealize Automation et JSON](#)

À propos de l'installation silencieuse de vRealize Automation

L'installation silencieuse de vRealize Automation utilise un fichier exécutable qui fait référence à un fichier texte de réponses.

Dans le fichier de réponses, vous préconfigurez les noms de domaine complets du système, les informations d'identification de compte et d'autres paramètres que vous ajoutez généralement tout au long d'une installation traditionnelle basée sur assistant ou manuelle. L'installation silencieuse s'avère utile pour les types de déploiement suivants :

- Déploiement de nombreux environnements quasiment identiques
- Redéploiements répétés du même environnement
- Installations sans assistance
- Installations avec scripts

Effectuer une installation silencieuse de vRealize Automation

Vous pouvez effectuer une installation silencieuse sans assistance de vRealize Automation à partir de la console d'un dispositif vRealize Automation nouvellement déployé.

Conditions préalables

- Créer un dispositif non configuré. Reportez-vous à [Déployer le dispositif vRealize Automation](#).
- Créez ou identifiez vos serveurs Windows IaaS et configurez leurs conditions préalables.
- Installez l'agent de gestion sur vos serveurs Windows IaaS.

Vous pouvez installer l'agent de gestion à l'aide du fichier téléchargé `.msi` traditionnel ou à l'aide du processus silencieux décrit dans la section [Effectuer une installation silencieuse de l'agent de gestion de vRealize Automation](#).

Procédure

- 1 Connectez-vous à la console du dispositif vRealize Automation en tant qu'utilisateur racine.

- 2 Accédez au répertoire suivant :

```
/usr/lib/vcac/tools/install
```

- 3 Ouvrez le fichier de réponses `ha.properties` dans un éditeur de texte.

- 4 Ajoutez les entrées spécifiques à votre déploiement dans le fichier `ha.properties`, puis enregistrez et fermez le fichier.

Vous pouvez également gagner du temps en copiant et en modifiant un fichier `ha.properties` d'un autre déploiement au lieu de modifier l'ensemble du fichier par défaut.

- 5 Démarrez l'installation à partir du même annuaire en exécutant la commande suivante :

```
vra-ha-config.sh
```

L'installation peut prendre jusqu'à une heure, voire plus, selon l'environnement et la taille du déploiement.

- 6 (Facultatif) Une fois l'installation terminée, examinez le fichier journal :

```
/var/log/vcac/vra-ha-config.log.
```

Le programme d'installation silencieuse n'enregistre pas les données exclusives, telles que les mots de passe, licences ou certificats, dans le journal.

Effectuer une installation silencieuse de l'agent de gestion de vRealize Automation

Vous pouvez effectuer une ligne de commande basée sur l'installation de l'agent de gestion de vRealize Automation sur n'importe quel serveur Windows IaaS.

L'installation silencieuse de l'agent de gestion se compose d'un script Windows PowerShell dont vous personnalisez quelques paramètres. Après avoir ajouté les paramètres spécifiques à votre déploiement, vous pouvez installer silencieusement l'agent de gestion sur tous vos serveurs Windows IaaS en exécutant des copies du même script sur chacun d'eux.

Conditions préalables

- Créer un dispositif non configuré. Reportez-vous à [Déployer le dispositif vRealize Automation](#).
- Créez ou identifiez vos serveurs Windows IaaS et configurez leurs conditions préalables.

Procédure

- 1 Connectez-vous au serveur IaaS Windows en utilisant un compte ayant des droits d'administrateur.
- 2 Ouvrez un navigateur Web à l'URL du programme d'installation de vRealize Automation.
`https://vrealize-automation-appliance-FQDN:5480/installer`
- 3 Cliquez avec le bouton droit sur le fichier de script PowerShell `InstallManagementAgent.ps1` et enregistrez-le sur le bureau ou dans un dossier du serveur Windows IaaS.
- 4 Ouvrez `InstallManagementAgent.ps1` dans un éditeur de texte.
- 5 Vers le haut du fichier de script, ajoutez les paramètres spécifiques à votre déploiement.
 - URL du dispositif vRealize Automation
`https://vrealize-automation-appliance-FQDN:5480`
 - Informations d'identification du compte d'utilisateur racine du dispositif vRealize Automation
 - Informations d'identification de l'utilisateur du service vRealize Automation, un compte de domaine avec privilèges d'administrateur sur les serveurs Windows IaaS
 - Dossier dans lequel vous voulez installer l'agent de gestion, `Program Files (x86)` par défaut
 - (Facultatif) Empreinte numérique du certificat au format PEM que vous utilisez pour l'authentification
- 6 Enregistrez et fermez le fichier `InstallManagementAgent.ps1`.
- 7 Pour installer silencieusement l'agent de gestion, double-cliquez sur `InstallManagementAgent.ps1`.
- 8 (Facultatif) Assurez-vous que l'installation s'est achevée en localisant l'**agent de gestion de VMware vCloud Automation Center** dans la liste Programmes et fonctionnalités du panneau de configuration Windows, et dans la liste des services Windows qui s'exécutent.

Fichier de réponses pour installation silencieuse de vRealize Automation

Les installations silencieuses de vRealize Automation nécessitent la préparation préalable d'un fichier texte de réponses.

Tous les dispositifs vRealize Automation qui viennent d'être déployés contiennent un fichier de réponses par défaut :

`/usr/lib/vcac/tools/install/ha.properties`.

Pour effectuer une installation silencieuse, vous devez utiliser un éditeur de texte pour personnaliser les paramètres du fichier `ha.properties` et adapter ces derniers au déploiement souhaité. Les exemples suivants présentent certains des paramètres et informations que vous devez ajouter.

- Votre clé de licence vRealize Automation ou de suite logicielle
- Noms de domaine complets des nœuds dispositif vRealize Automation
- Informations d'identification du compte d'utilisateur racine de dispositif vRealize Automation
- Noms de domaine complets des serveurs Windows IaaS qui feront office de nœuds Web, de nœuds Manager Service, etc.
- Informations d'identification de l'utilisateur du service vRealize Automation, un compte de domaine avec privilèges d'administrateur sur les serveurs Windows IaaS
- Noms de domaine complets des équilibres de charge
- Paramètres de la base de données SQL Server
- Paramètres d'agent proxy pour la connexion aux ressources de virtualisation
- Indique si le programme d'installation silencieuse doit tenter de corriger les conditions préalables manquantes du serveur Windows IaaS

Le programme d'installation silencieuse peut corriger de nombreuses conditions préalables Windows manquantes. Cependant, il ne peut pas corriger certains problèmes de configuration (comme un nombre insuffisant de CPU).

Pour gagner du temps, vous pouvez réutiliser et modifier un fichier `ha.properties` configuré pour un autre déploiement dont les paramètres étaient semblables. En outre, lorsque vous installez vRealize Automation de façon non silencieuse par le biais de l'assistant d'installation, l'assistant crée vos paramètres et les enregistre dans le fichier `ha.properties`. Ce fichier peut être utile pour effectuer des modifications en vue d'une réutilisation lors de l'installation silencieuse d'un déploiement semblable.

L'assistant n'enregistre pas les paramètres exclusifs, tels que les mots de passe, licences ou certificats, dans le fichier `ha.properties`.

La ligne de commande d'installation de vRealize Automation

vRealize Automation inclut une interface de ligne de commande basée sur une console pour l'exécution de réglages d'installation pouvant être requis après l'installation initiale.

L'interface de ligne de commande (CLI) peut exécuter des tâches d'installation et de configuration qui ne sont plus disponibles par le biais de l'interface basée sur le navigateur après l'installation initiale. Les fonctionnalités CLI incluent la vérification des conditions préalables, l'installation de composants IaaS, l'installation de certificats ou la définition du nom d'hôte vRealize Automation vers lequel les utilisateurs pointent leur navigateur Web.

L'interface de ligne de commande est également utile aux utilisateurs avancés qui souhaitent exécuter certaines opérations au moyen d'un script. Certaines fonctions de l'interface de ligne de commande sont utilisées par l'installation silencieuse, il convient donc de vous familiariser avec les deux fonctions pour renforcer vos connaissances sur l'écriture d'un script d'installation de vRealize Automation.

vRealize Automation Notions de base sur l'installation depuis la ligne de commande

L'interface de ligne de commande d'installation de vRealize Automation inclut des opérations de base de niveau supérieur.

Les opérations de base affichent les ID de nœud de vRealize Automation, exécutent des commandes, indiquent l'état des commandes ou affichent les informations d'aide. Pour présenter ces opérations et leurs options sur l'affichage de la console, entrez la commande suivante sans option ni qualificatif.

```
vra-command
```

Afficher les ID de nœud

Il vous faut les ID de nœud vRealize Automation pour exécuter des commandes sur les systèmes cibles appropriés. Pour afficher les ID de nœud, entrez la commande suivante.

```
vra-command list-nodes
```

Notez les ID des nœuds avant d'exécuter des commandes sur des machines spécifiques.

Exécuter des commandes

La plupart des fonctions de ligne de commande impliquent l'exécution d'une commande sur un nœud dans le cluster vRealize Automation. Pour exécuter une commande, utilisez la syntaxe suivante.

```
vra-command execute --node node-ID command-name --parameter-name parameter-value
```

Comme le montre la syntaxe précédente, de nombreuses commandes nécessitent des paramètres et des valeurs de paramètres sélectionnés par l'utilisateur.

Afficher l'état d'une commande

Certaines commandes s'exécutent en quelques instants, d'autres sont plus longues. Pour surveiller l'avancement d'une commande qui a été soumise, entrez la commande suivante.

```
vra-command status
```

L'état de la commande est particulièrement pratique pour surveiller une installation silencieuse qui peut se prolonger pour les déploiements de grande taille.

Afficher l'aide

Pour afficher l'aide sur toutes les commandes disponibles, entrez la commande suivante.

```
vra-command help
```

Pour afficher de l'aide sur une commande spécifique, entrez la commande suivante.

```
vra-command help command-name
```

Noms des commandes d'installation de vRealize Automation

Les commandes vous donnent un accès par la console à de nombreuses tâches d'installation et de configuration de vRealize Automation que vous pouvez exécuter après l'installation initiale.

Les commandes disponibles mettent notamment en œuvre les fonctions suivantes.

- Ajout d'un autre dispositif vRealize Automation à une installation existante
- Définition du nom de l'hôte vers lequel les utilisateurs dirigent le navigateur Web lorsqu'ils accèdent à vRealize Automation
- Création de la base de données IaaS SQL Server
- Exécution de l'outil de vérification des conditions préalables sur un serveur IaaS Windows
- Importation de certificats

Pour la liste complète des commandes vRealize Automation disponibles, connectez-vous à la console du dispositif vRealize Automation, puis entrez la commande suivante.

```
vra-command help
```

La longue liste de noms de commandes et de paramètres n'est pas reproduite dans une documentation distincte. Pour utiliser la liste efficacement, identifiez une commande qui vous intéresse, puis ciblez de façon plus précise la demande en entrant la commande suivante.

```
vra-command help command-name
```

API d'installation de vRealize Automation

L'API REST de vRealize Automation pour l'installation vous donne la possibilité de créer des installations purement contrôlées par logiciel pour vRealize Automation.

L'API d'installation nécessite une version au format JSON des mêmes entrées qu'obtient l'installation depuis l'interface de ligne de commande à partir du fichier de réponse `ha.properties`. Les directives suivantes vous permettent de vous familiariser avec le fonctionnement de l'API. Vous pourrez ensuite concevoir des appels programmatiques de conception à l'API pour installer vRealize Automation.

- Pour accéder à la documentation de l'API, accédez à la page Web du dispositif vRealize Automation suivante.

`https://vrealize-automation-appliance-FQDN:5480/config`

Vous avez besoin d'un dispositif vRealize Automation non configuré. Reportez-vous à [Déployer le dispositif vRealize Automation](#).

- Pour expérimenter l'installation basée sur API, localisez et développez la commande PUT suivante.

`PUT /vra-install`

- Copiez le format JSON non renseigné de la zone **install_json** vers un éditeur de texte. Renseignez les valeurs de réponse de la même manière que vous le feriez pour `ha.properties`. Lorsque vos réponses au format JSON sont prêtes, recopiez le code dans **install_json** et remplacez le format JSON non renseigné.

Vous pouvez également modifier le modèle JSON suivant et copier les résultats dans **install_json**.

`/usr/lib/vcac/tools/install/installationProperties.json`

Vous pouvez également convertir un `ha.properties` renseigné en JSON ou vice versa.

- Dans la zone d'action, sélectionnez **validate** et cliquez sur **Try It Out**.

L'action de validation exécute l'utilitaire de vérification et de correction des conditions requises de vRealize Automation.

- La réponse de validation inclut un ID de commande alphanumérique que vous pouvez insérer dans la commande GET suivante.

`GET /commands/command-id/aggregated-status`

La réponse au GET inclut l'avancement de l'opération de validation.

- Lorsque la validation aboutit, vous pouvez exécuter l'installation proprement dite en recommençant le processus. Dans la zone d'action, sélectionnez simplement **install** plutôt que **validate**.

L'installation peut prendre un certain temps selon la taille du déploiement. De nouveau, localisez l'ID de commande, puis utilisez la commande GET d'état agrégé pour obtenir l'avancement de l'installation. La réponse GET peut ressembler à l'exemple suivant.

```
"progress": "78%", "counts": {"failed": 0, "completed": 14, "total": 18,
"queued": 3, "processing": 1}, "failed-commands": 0
```

- Si l'installation ne se déroule pas correctement, vous pouvez déclencher une collecte de journaux pour tous les nœuds à l'aide de la commande suivante.

```
PUT /commands/log-bundle
```

À l'instar de l'installation, l'ID de commande alphanumérique renvoyé vous permet de surveiller l'état de collecte de journaux.

Convertir entre propriétés silencieuses vRealize Automation et JSON

Pour les installations silencieuses de vRealize Automation avec l'interface de ligne de commande ou pour les installations basées sur API, vous pouvez convertir un fichier de réponse de propriétés renseigné en JSON ou vice versa. L'installation silencieuse sur interface de ligne de commande nécessite le fichier de propriétés, tandis que l'API nécessite un format JSON.

Conditions préalables

Un fichier de réponse de propriétés renseigné ou un fichier JSON renseigné

```
/usr/lib/vcac/tools/install/ha.properties.
```

ou

```
/usr/lib/vcac/tools/install/installationProperties.json
```

Procédure

- 1 Connectez-vous à une session de console de dispositif vRealize Automation en tant qu'utilisateur racine.
- 2 Exécutez le script de convertisseur approprié.

- Convertissez JSON en propriétés

```
/usr/lib/vcac/tools/install/convert-properties --from-json  
installationProperties.json
```

Le script crée un nouveau fichier de propriétés avec un nom incluant l'horodatage, par exemple :

```
ha.2016-10-17_13.02.15.properties
```

- Convertir des propriétés en JSON

```
/usr/lib/vcac/tools/install/convert-properties --to-json ha.properties
```

Le script crée un nouveau fichier `installationProperties.json` avec un nom incluant l'horodatage, par exemple :

```
installationProperties.2016-10-17_13.36.13.json
```

Résultats

Vous pouvez également afficher de l'aide pour le script.

```
/usr/lib/vcac/tools/install/convert-properties --help
```

Tâches post-installation vRealize Automation

7

Après avoir installé vRealize Automation, vous devrez éventuellement effectuer des tâches post-installation.

Ce chapitre contient les rubriques suivantes :

- [Ne pas modifier le fuseau horaire vRealize Automation](#)
- [Configurer le chiffrement conforme à la norme de traitement des informations fédérales](#)
- [Activer le basculement automatique de Manager Service](#)
- [Basculement de la base de données PostgreSQL vRealize Automation automatique](#)
- [Remplacement de certificats autosignés par des certificats fournis par une autorité](#)
- [Modification de noms d'hôtes et d'adresses IP](#)
- [Supprimer un nœud du dispositif vRealize Automation](#)
- [Installation de l'agent vRealize Log Insight sur des serveurs IaaS](#)
- [Modifier le port de proxy de VMware Remote Console](#)
- [Modifier un nom de domaine complet du dispositif vRealize Automation et lui attribuer le nom de domaine complet d'origine](#)
- [Configurer le groupe de disponibilité AlwaysOn SQL](#)
- [Ajouter des contrôleurs d'interface réseau après l'installation de vRealize Automation](#)
- [Configurer des routes statiques](#)
- [Gestion des correctifs accés](#)
- [Configurer l'accès au locataire par défaut](#)

Ne pas modifier le fuseau horaire vRealize Automation

Même si l'interface de gestion du dispositif vRealize Automation fournit une option pour la modifier, laissez toujours le fuseau horaire vRealize Automation défini sur Etc/UTC.

L'utilisation d'un fuseau horaire autre qu'Etc/UTC peut provoquer des erreurs inhabituelles telles que l'échec de migrations et des bundles de journaux qui ne contiennent pas les entrées provenant de tous les nœuds vRealize Automation.

L'option de l'interface de gestion du dispositif vRealize Automation que vous devez éviter se trouve sous **Système > Fuseau horaire**.

Configurer le chiffrement conforme à la norme de traitement des informations fédérales

Vous pouvez activer ou désactiver le chiffrement conforme à la norme FIPS (Federal Information Processing Standard) 140–2 pour le trafic réseau entrant et sortant du dispositif vRealize Automation.

La modification du paramètre FIPS nécessite un redémarrage de vRealize Automation. FIPS est désactivé par défaut.

Procédure

- 1 Connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.

`https://vrealize-automation-appliance-FQDN:5480`

- 2 Cliquez sur **vRA > Paramètres de l'hôte**.

- 3 À proximité de l'angle droit supérieur, cliquez sur le bouton permettant d'activer ou de désactiver FIPS.

Lorsqu'il est activé, le trafic réseau entrant et sortant du dispositif vRealize Automation sur le port 443 utilise le chiffrement conforme à FIPS 140–2. Quel que soit le paramètre FIPS, vRealize Automation utilise des algorithmes conformes à AES–256 pour protéger les données sécurisées stockées sur le dispositif vRealize Automation.

Note Cette version de vRealize Automation assure uniquement partiellement la conformité FIPS, car certains composants internes n'utilisent pas encore des modules de chiffrement certifiés. Lorsque les modules certifiés n'ont pas encore été mis en œuvre, les algorithmes conformes à AES–256 sont utilisés.

- 4 Cliquez sur **Oui** pour redémarrer vRealize Automation.

Résultats

Vous pouvez également configurer FIPS à partir d'une session de console de dispositif vRealize Automation en tant qu'utilisateur racine en utilisant les commandes suivantes.

```
vcac-vami fips enable
vcac-vami fips disable
vcac-vami fips status
```

Activer le basculement automatique de Manager Service

Le basculement automatique de Manager Service est désactivé par défaut si vous installez ou mettez à niveau Manager Service avec le programme d'installation de Windows vRealize Automation standard.

Pour activer le basculement automatique de Manager Service après avoir exécuté le programme d'installation standard de Windows, procédez comme suit.

Dans une configuration à plusieurs nœuds, vous n'avez besoin d'effectuer les étapes qu'une seule fois, sur n'importe quel nœud de dispositif vRealize Automation.

Procédure

- 1 Connectez-vous en tant qu'utilisateur racine à une session de console sur le dispositif vRealize Automation.

- 2 Accédez au répertoire suivant :

```
/usr/lib/vcac/tools/vami/commands
```

- 3 Entrez la commande suivante :

```
python ./manager-service-automatic-failover ENABLE
```

Résultats

Si vous devez désactiver le basculement automatique dans un déploiement IaaS, entrez la commande suivante à la place.

```
python ./manager-service-automatic-failover DISABLE
```

À propos du basculement automatique de Manager Service

Vous pouvez configurer vRealize Automation IaaS Manager Service pour basculer automatiquement sur une sauvegarde si l'instance principale de Manager Service s'arrête.

À partir de vRealize Automation 7.3, vous n'avez plus besoin de démarrer ou d'arrêter Manager Service manuellement sur chaque serveur Windows pour contrôler lequel est utilisé comme serveur principal ou de secours. Le basculement automatique de Manager Service est activé par défaut dans les cas suivants.

- Lorsque vous installez vRealize Automation en mode silencieux ou avec l'assistant d'installation
- Lorsque vous mettez à niveau IaaS via l'interface d'administration ou avec le script de mise à niveau automatique.

Le basculement n'est pas activé lorsque le programme d'installation basé sur Windows standard permet d'ajouter un hôte Manager Service ou de mettre à niveau IaaS. Pour l'activer, consultez [Activer le basculement automatique de Manager Service](#).

Lorsque le basculement automatique est activé, Manager Service démarre automatiquement sur tous les hôtes Manager Service, y compris les sauvegardes. La fonctionnalité de basculement automatique permet aux hôtes de se surveiller mutuellement de manière transparente et de basculer si nécessaire. La fonctionnalité requiert que le service Windows soit en cours d'exécution sur tous les hôtes.

Note Vous n'êtes pas obligé d'utiliser le basculement automatique. Vous pouvez le désactiver et continuer de démarrer et d'arrêter manuellement le service Windows pour contrôler quel hôte sert d'hôte principal ou de sauvegarde. Si vous choisissez le basculement manuel, il vous suffit de démarrer le service sur un hôte à la fois. Avec le basculement automatique désactivé, l'exécution simultanée du service sur plusieurs serveurs IaaS rend vRealize Automation inutilisable.

Ne tentez pas d'activer ou de désactiver de manière sélective le basculement automatique. Le basculement automatique doit toujours être synchronisé, qu'il soit sous tension ou hors tension, sur chaque hôte Manager Service dans un déploiement IaaS.

Si le basculement automatique ne semble pas fonctionner, reportez-vous à *Mise à niveau depuis vRealize Automation 7.1 ou 7.2 vers la version 7.3* pour obtenir des conseils sur le dépannage.

Pour plus d'informations sur la façon d'équilibrer la charge de travail d'hôtes Manager Service, reportez-vous à [Équilibrage de charge de vRealize Automation](#).

Basculement de la base de données PostgreSQL vRealize Automation automatique

Dans un déploiement vRealize Automation à haute disponibilité, certaines configurations autorisent la base de données PostgreSQL vRealize Automation intégrée à basculer automatiquement.

Le basculement automatique est activé en mode silencieux dans les conditions suivantes.

- Le déploiement haute disponibilité inclut trois dispositifs vRealize Automation.
Le basculement automatique n'est pas pris en charge avec seulement deux dispositifs.
- La réplication de la base de données est définie sur le mode synchrone sous l'onglet Cluster de l'interface d'administration de vRealize Automation.

En règle générale, évitez d'effectuer un basculement manuel alors que le basculement automatique est activé. Toutefois, en cas de problèmes de nœud, le basculement automatique peut ne pas se produire même s'il est activé. Le cas échéant, vérifiez si vous avez besoin d'effectuer un basculement manuel.

- 1 Une fois que le nœud de base de données PostgreSQL principal échoue, attendez jusqu'à 5 minutes pour que le reste du cluster se stabilise.
- 2 Sur un nœud de dispositif vRealize Automation encore fonctionnel, ouvrez un navigateur avec l'URL suivante.

`https://vrealize-automation-appliance-FQDN:5434/api/status`

3 Recherchez `manualFailoverNeeded`.

4 Si `manualFailoverNeeded` est vraie, effectuez un basculement manuel.

Pour plus d'informations sur l'exécution d'un basculement manuel, reportez-vous à la section *Gestion de vRealize Automation*.

Remplacement de certificats autosignés par des certificats fournis par une autorité

Si vous avez installé vRealize Automation avec des certificats autosignés, vous pouvez décider de les remplacer par des certificats fournis par une autorité de certification avant d'effectuer un déploiement dans un environnement de production.

Pour plus d'informations sur la mise à jour des certificats, reportez-vous à la section *Gestion de vRealize Automation*.

Modification de noms d'hôtes et d'adresses IP

En règle générale, il est recommandé de conserver les noms d'hôtes, les noms de domaine complets et les adresses IP que vous avez prévu d'utiliser pour les systèmes vRealize Automation. Certaines modifications post-installation sont possibles, mais peuvent s'avérer complexes.

- Si vous modifiez le nom d'hôte de la machine Windows qui héberge la base de données SQL Server IaaS, reportez-vous à la section *Gestion de vRealize Automation*.
- Lors de la restauration des composants IaaS, le fait de renommer un hôte peut affecter l'hôte IaaS Web, l'hôte Manager Service ou leurs équilibrages de charge respectifs. Restaurez ces hôtes ou ces équilibrages de charge en fonction de la sauvegarde de *vRealize Suite* et des instructions de restauration.

Pour modifier le nom d'hôte ou l'adresse IP d'un dispositif vRealize Automation, reportez-vous aux sections suivantes.

Modifier le nom d'hôte du dispositif vRealize Automation

Lors de la maintenance d'un environnement ou d'un réseau, vous devrez éventuellement attribuer un nom d'hôte différent à un dispositif vRealize Automation.

Important Le changement de nom met vRealize Automation hors ligne pendant plusieurs minutes.

Les mêmes étapes s'appliquent aux dispositifs vRealize Automation autonomes, maîtres et réplicas.

Procédure

- 1 Dans DNS, créez un enregistrement supplémentaire avec le nouveau nom d'hôte du nœud.
Ne supprimez pas l'enregistrement DNS portant l'ancien nom d'hôte pour l'instant.
- 2 Attendez la réplication DNS et la distribution de zone.
- 3 Connectez-vous à la ligne de commande du dispositif vRealize Automation en tant qu'utilisateur racine.
- 4 Exécutez la commande suivante.

```
vcac-config hostname-change --host new-hostname --certificate certificate-file-name
```

Un fichier de certificat est facultatif, sauf si l'ancien nom d'hôte de dispositif a été utilisé dans un certificat. Si c'est le cas, fournissez un certificat mis à jour comprenant le nouveau nom d'hôte.

Lorsque vous spécifiez un fichier de certificat, la commande de changement de nom importe également le certificat et renvoie son ID.

Un fichier de certificat doit être au même format que la sortie de texte de la commande d'API `/config/ssl/generate-certificate` et contenir le nouveau nom DNS dans son champ SAN.

- 5 Patientez 15 minutes ou plus jusqu'à la fin du processus de changement de nom. Les actions de commande prennent quelques minutes, suivies de plusieurs minutes supplémentaires de réinscription du service.
- 6 Si l'ancien nom d'hôte de dispositif a été utilisé avec un équilibrage de charge dans un environnement HA, vérifiez et reconfigurez l'équilibrage de charge avec le nouveau nom.
- 7 Dans DNS, supprimez l'ancien enregistrement DNS portant l'ancien nom d'hôte.

Résultats

Si vous avez des difficultés pour changer un nom d'hôte, essayez plutôt les procédures distinctes de la documentation de vRealize Automation 7.3.

Modifier l'adresse IP du dispositif vRealize Automation

Lors de la maintenance d'un environnement ou d'un réseau, vous devrez éventuellement attribuer une adresse IP différente à un dispositif vRealize Automation existant.

Conditions préalables

- Par précaution, prenez des snapshots des dispositifs vRealize Automation et des serveurs IaaS.
- À partir d'une session de console en tant qu'utilisateur racine sur les dispositifs vRealize Automation, inspectez les entrées du fichier `/etc/hosts`.

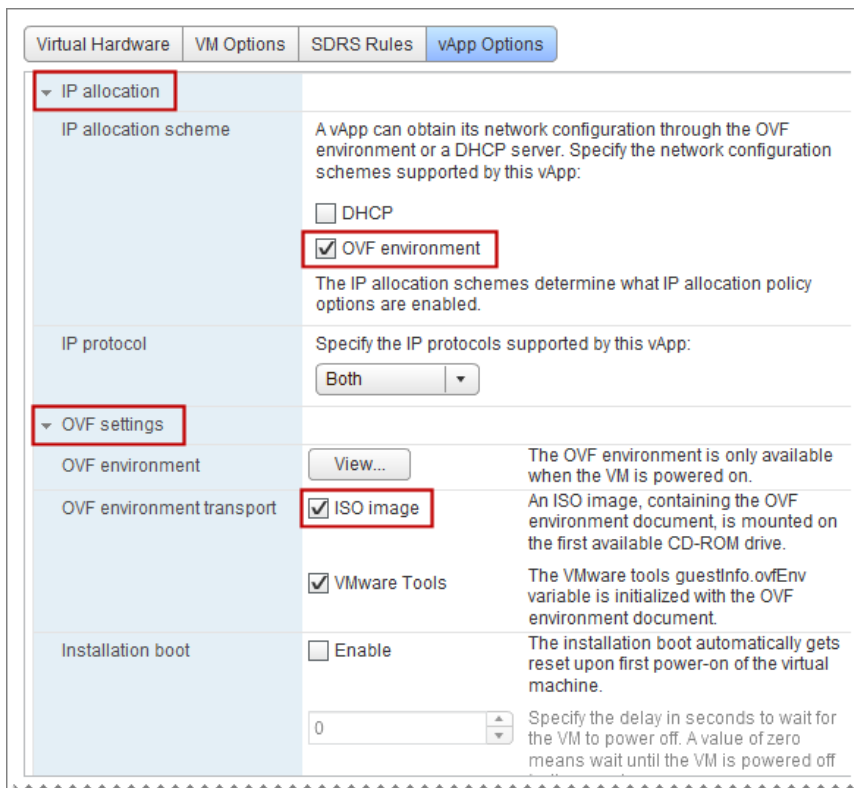
Recherchez les attributions d'adresses pouvant entrer en conflit avec le nouveau plan d'adressage IP et apportez les modifications nécessaires.

Sur tous les serveurs IaaS, répétez la procédure pour le fichier `Windows\system32\drivers\etc\hosts`.

- Arrêtez tous les dispositifs vRealize Automation.
- Arrêtez tous les services vRealize Automation sur les serveurs IaaS.

Procédure

- 1 Dans vSphere, localisez le dispositif vRealize Automation que vous souhaitez modifier et sélectionnez **Actions > Modifier les paramètres**.
- 2 Cliquez sur **Options vApp**.
- 3 Développez **Allocation d'adresses IP** et activez l'option **Environnement OVF**.
- 4 Développez **Paramètres OVF** et activez l'option **Image ISO**.



- 5 Cliquez sur **OK**.
- 6 Démarrez le dispositif vRealize Automation que vous modifiez.
- 7 Connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.
`https://vrealize-automation-appliance-FQDN:5480`
- 8 Cliquez sur l'onglet **Réseau**.
- 9 Sous les onglets, cliquez sur **Adresse**.

- 10 Mettez à jour l'adresse IP.
- 11 Dans le coin supérieur droit, cliquez sur **Enregistrer les paramètres**.
- 12 Arrêtez le dispositif vRealize Automation que vous modifiez.
- 13 Dans DNS, mettez à jour les entrées des nouvelles adresses IP.

Mettez uniquement à jour les enregistrements de type A existants. Ne modifiez pas les noms de domaine complets.

Si vous utilisez un équilibrage de charge, mettez également à jour les paramètres IP d'équilibrage de charge pour les nœuds principaux, les pools de service et les serveurs virtuels selon les besoins.

- 14 Attendez la réplication DNS et la distribution de zone.
- 15 Démarrez tous les dispositifs vRealize Automation.
- 16 Démarrez les services vRealize Automation sur les serveurs IaaS.
- 17 Connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.

`https://vrealize-automation-appliance-FQDN:5480`

- 18 Vérifiez l'état du dispositif vRealize Automation dans les zones suivantes.

- État de la connexion à la base de données sous **Cluster**
- État de RabbitMQ sous **vRA > Messagerie**
- État de Xenon sous **vRA > Xenon**
- Tous les services ENREGISTRÉ sous **Services**

Ajuster la base de données SQL pour un nom d'hôte modifié

Vous devez réviser les paramètres de configuration si vous déplacez la base de données SQL vRealize AutomationIaaS vers un autre nom d'hôte.

Sur le même nom d'hôte, vous pouvez restaurer la base de données SQL à partir d'une sauvegarde, sans étapes supplémentaires requises. Si vous effectuez une restauration vers un nom d'hôte différent, vous devez modifier les fichiers de configuration afin d'apporter des modifications supplémentaires.

Consultez [Article 2074607 de la base de connaissances VMware](#) pour les modifications requises lors du déplacement de la base de données SQL vers un nom d'hôte différent.

Modifier l'adresse IP d'un serveur IaaS

Lors de la maintenance d'un environnement ou d'un réseau, vous devrez éventuellement attribuer une adresse IP différente à un serveur Windows vRealize AutomationIaaS existant.

Conditions préalables

- Si l'adresse IP du dispositif vRealize Automation doit être modifiée, effectuez d'abord cette modification. Reportez-vous à [Modifier l'adresse IP du dispositif vRealize Automation](#).
- Par précaution, prenez des snapshots des dispositifs vRealize Automation et des serveurs IaaS.
- À partir d'une session de console en tant qu'utilisateur racine sur le dispositif vRealize Automation, inspectez les entrées du fichier `/etc/hosts`.

Recherchez les attributions d'adresses pouvant entrer en conflit avec le nouveau plan d'adressage IP et apportez les modifications nécessaires.

Sur tous les serveurs IaaS, répétez la procédure pour le fichier `Windows\system32\drivers\etc\hosts`.

- Arrêtez le dispositif vRealize Automation.
- Arrêtez tous les services vRealize Automation sur les serveurs IaaS.

Procédure

- 1 Connectez-vous au serveur IaaS en utilisant un compte ayant des droits d'administrateur.

- 2 Dans Windows, modifiez l'adresse IP.

Recherchez l'adresse IP dans la fenêtre Paramètres de l'adaptateur réseau Windows, sous les propriétés du protocole Internet.

- 3 Actualisez votre DNS local avec les modifications.

L'actualisation de DNS garantit que les serveurs Windows IaaS peuvent se trouver et que vous pouvez vous reconnecter à un serveur Windows si vous êtes déconnecté.

- 4 Sur l'hôte Manager Service, examinez le fichier suivant dans un éditeur de texte.

`install-folder\VCAC\Server\ManagerService.exe.config`

Le dossier d'installation par défaut est `C:\Program Files (x86)\VMware`.

Vérifiez les adresses IP ou les noms de domaine complets des dispositifs vRealize Automation et des serveurs Windows IaaS.

- 5 Sur tous les serveurs Windows IaaS, examinez le fichier suivant dans un éditeur de texte.

`install-folder\VCAC\Management Agent\VMware.IaaS.Management.Agent.exe.Config`

Vérifiez l'adresse IP ou le nom de domaine complet du dispositif vRealize Automation.

- 6 Connectez-vous à l'hôte SQL Server.

- 7 Vérifiez que l'adresse du référentiel est correctement configurée pour utiliser le nom de domaine complet dans la colonne `ConnectionString`.

Par exemple, ouvrez SQL Management Studio et exécutez la requête suivante.

```
"SELECT Name, ConnectionString FROM [database-name].[DynamicOps.RepositoryModel].[Models]"
```


- 8 Démarrez le dispositif vRealize Automation.
- 9 Démarrez les services vRealize Automation sur les serveurs IaaS.
- 10 Examinez les fichiers journaux pour vérifier que les services d'agent, de DEM Worker, de Manager Service et d'hôte Web ont bien démarré.
- 11 Connectez-vous à vRealize Automation en tant qu'utilisateur disposant du rôle d'administrateur d'infrastructure.
- 12 Accédez à **Infrastructure > Surveillance > État d'exécution distribuée** et vérifiez que tous les services sont en cours d'exécution.
- 13 Testez le bon fonctionnement en vérifiant les services de dispositif, en testant le provisionnement, ou en utilisant l'outil de test de production vRealize.

Modifier un nom d'hôte de serveur IaaS

Lors de la maintenance d'un environnement ou d'un réseau, vous devrez éventuellement attribuer un nom d'hôte différent à un serveur Windows vRealize Automation IaaS existant.

Procédure

- 1 Prenez un snapshot du serveur IaaS.
- 2 Sur le serveur IaaS, utilisez IIS Manager pour arrêter les pools d'applications vRealize Automation : Repository, VMware vRealize Automation et Wapi.
- 3 Sur le serveur IaaS, utilisez les Outils administrateur > Services pour arrêter tous les services, agents et DEM vRealize Automation.
- 4 Dans DNS, créez un enregistrement supplémentaire avec le nouveau nom d'hôte.
Ne supprimez pas l'enregistrement DNS portant l'ancien nom d'hôte pour l'instant.
- 5 Attendez la réplication DNS et la distribution de zone.
- 6 Sur le serveur IaaS, modifiez le nom d'hôte mais ne redémarrez pas lorsque vous y êtes invité.
Recherchez le nom d'hôte dans les propriétés du système Windows, sous le nom de l'ordinateur, le domaine et les paramètres du groupe de travail.
Lorsque vous êtes invité à redémarrer, cliquez sur l'option pour redémarrer plus tard.
- 7 Si vous avez utilisé l'ancien nom d'hôte pour générer des certificats, mettez à jour les certificats.
Pour obtenir des informations sur la mise à jour des certificats, consultez la section *Gestion de vRealize Automation*.

- 8 Utilisez un éditeur de texte pour localiser et mettre à jour le nom d'hôte à l'intérieur des fichiers de configuration.

Effectuez les mises à jour en fonction du nom d'hôte du serveur IaaS que vous avez modifié. Dans un déploiement distribué HA, vous devrez peut-être accéder à plusieurs serveurs. Il n'existe aucune mise à jour si vous modifiez le nom d'hôte d'un composant DEM Orchestrator ou DEM Worker.

Note Mettre à jour uniquement l'ancien nom d'hôte de serveur Windows. Si à la place, vous trouvez un nom d'équilibrage de charge, conservez-le.

Tableau 7-1. Fichiers à mettre à jour lorsque vous modifiez un nom d'hôte du nœud Web

Serveur IaaS	Chemin d'accès	Fichier
Nœuds Web	<i>install-folder\Server\Website</i>	Web.config
	<i>install-folder\Server\Website\Cafe</i>	Vcac-Config.exe.config
	<i>install-folder\Web API</i>	Web.config
	<i>install-folder\Web API\ConfigTool</i>	Vcac-Config.exe.config
Nœud avec le composant Model Manager installé	<i>install-folder\Server\Model Manager Data</i>	Repoutil.exe.config
	<i>install-folder\Server\Model Manager Data\Cafe</i>	Vcac-Config.exe.config
Nœuds Manager Service	<i>install-folder\Server</i>	ManagerService.exe.config
Nœuds DEM Orchestrator	<i>install-folder\Distributed Execution Manager\dem</i>	DynamicOps.DEM.exe.config
Nœuds DEM Worker	<i>install-folder\Distributed Execution Manager\DEM-name</i>	DynamicOps.DEM.exe.config
Nœuds Agent	<i>install-folder\Agents\agent-name</i>	RepoUtil.exe.config
	<i>install-folder\Agents\agent-name</i>	VRMAgent.exe.config

Tableau 7-2. Fichiers à mettre à jour lorsque vous modifiez un nom d'hôte du nœud Manager Service

Serveur IaaS	Chemin d'accès	Fichier
Nœuds DEM Orchestrator	<i>install-folder\Distributed Execution Manager\DEM-name</i>	DynamicOps.DEM.exe.config
Nœuds DEM Worker	<i>install-folder\Distributed Execution Manager\dem</i>	DynamicOps.DEM.exe.config
Nœuds Agent	<i>install-folder\Agents\agent-name</i>	VRMAgent.exe.config

Tableau 7-3. Fichiers à mettre à jour lorsque vous modifiez un nom d'hôte du nœud Agent

Serveur IaaS	Chemin d'accès	Fichier
Nœud Agent	<i>install-folder\Agents\agent-name</i>	VRMAgent.exe.config

- 9 Redémarrez le serveur IaaS pour lequel vous avez modifié le nom d'hôte.
- 10 Démarrez les pools d'applications vRealize Automation que vous avez arrêtés précédemment.
- 11 Démarrez les services, les agents et les composants DEM vRealize Automation que vous avez arrêtés précédemment.
- 12 Si l'ancien nom d'hôte du serveur IaaS était utilisé avec un équilibrage de charge dans un environnement HA, vérifiez et reconfigurez l'équilibrage de charge avec le nouveau nom.
- 13 Dans DNS, supprimez l'ancien enregistrement DNS portant l'ancien nom d'hôte.
- 14 Attendez la réplication DNS et la distribution de zone.
- 15 Si vous avez modifié le nom d'un hôte Manager Service, exécutez les étapes supplémentaires suivantes.
 - a Mettez à jour les agents logiciels sur les machines virtuelles existantes.
 - b Recréez les images ISO ou les modèles qui contiennent un agent invité.

Étape suivante

Confirmer que vRealize Automation est prêt à être utilisé. Consultez la documentation de [Sauvegarde et restauration de vRealize Suite](#).

Définissez l'URL de connexion à vRealize Automation sur un nom personnalisé

Si vous souhaitez que les utilisateurs de vRealize Automation se connectent à un nom d'URL autre que le nom du dispositif vRealize Automation ou le nom de l'équilibrage de charge, suivez les étapes de personnalisation avant et après l'installation.

Procédure

- 1 Avant de procéder à l'installation, préparez un certificat qui inclut le CNAME que vous le souhaitez utiliser, ainsi que les noms du dispositif vRealize Automation et de l'équilibrage de charge.
- 2 Installez vRealize Automation, en entrant le nom du dispositif ou de l'équilibrage de charge comme d'habitude. Pendant l'installation, importez le certificat personnalisé.
- 3 Après l'installation, dans DNS, créez un alias CNAME Nom commun et pointez-le vers l'adresse VIP du dispositif ou de l'équilibrage de charge.

- 4 Connectez-vous à l'interface de l'administrateur de dispositif vRealize Automation en tant qu'utilisateur racine.

`https://vrealize-automation-appliance-FQDN:5480`

- 5 Sous **vRA > Paramètres de l'hôte**, remplacez le **Nom d'hôte** par le CNAME que vous avez choisi.

Supprimer un nœud du dispositif vRealize Automation

Lors de la maintenance d'un environnement HA, vous devrez peut-être supprimer un nœud du dispositif vRealize Automation défaillant à partir du cluster.

Pour supprimer un nœud, suivez les instructions de [Pour supprimer un dispositif, suivez les instructions de l'article 2149866 de la Base de connaissances VMware](#).

Installation de l'agent vRealize Log Insight sur des serveurs IaaS

Les serveurs Windows dans une configuration vRealize Automation IaaS n'incluent pas l'agent vRealize Log Insight par défaut.

vRealize Log Insight fournit une agrégation et une indexation de journaux, et peut collecter, importer et analyser des journaux pour exposer des problèmes du système. Si vous souhaitez capturer et analyser des journaux des serveurs IaaS en utilisant vRealize Log Insight, vous devez installer séparément l'agent vRealize Log Insight pour Windows.

Pour plus d'informations, reportez-vous au *guide d'administration de l'agent VMware vRealize Log Insight*.

Les dispositifs vRealize Automation incluent l'agent vRealize Log Insight par défaut.

Modifier le port de proxy de VMware Remote Console

Si votre site bloque ou réserve le port 8444, vous pouvez modifier le port de proxy par défaut utilisé par VMware Remote Console.

Procédure

- 1 Accédez à l'invite de commande du dispositif vRealize Automation en tant qu'utilisateur racine.
- 2 Ouvrez le fichier suivant dans un éditeur de texte.
`/etc/vcac/security.properties`
- 3 Remplacez la valeur par défaut 8444 de `consoleproxy.service.port` par un port inutilisé.
- 4 Enregistrez et fermez `security.properties`.
- 5 Redémarrez le dispositif vRealize Automation.

Résultats

Dans un environnement HA, apportez la même modification à tous les dispositifs vRealize Automation.

Modifier un nom de domaine complet du dispositif vRealize Automation et lui attribuer le nom de domaine complet d'origine

Dans certains cas, un nom de domaine complet du dispositif vRealize Automation peut changer lorsque vous ne le souhaitez pas. Par exemple, le nom de domaine complet change si vous créez un répertoire Integrated Windows Authentication (IWA) pour un domaine autre que le domaine sur lequel se trouve le dispositif.

Si vous créez un répertoire IWA pour un autre domaine, suivez les étapes suivantes pour modifier le nom de domaine complet du dispositif et lui attribuer le nom de domaine complet d'origine.

Procédure

- 1 Connectez-vous à vRealize Automation et créez l'annuaire IWA comme vous le feriez normalement.

Reportez-vous à *Configuration de vRealize Automation*.

- 2 S'il s'agit d'un environnement HA, suivez également les étapes à propos de la configuration de la gestion des annuaires pour HA dans le document *Configuration de vRealize Automation*.

- 3 La création d'un répertoire IWA pour un domaine autre que celui sur lequel se trouve un dispositif modifie discrètement le nom de domaine complet du dispositif.

Par exemple, va1.domain1.local devient va1.domain2.local lorsque vous créez un répertoire IWA pour domain2.local.

Annuler la modification en renommant chaque dispositif avec son nom de domaine complet d'origine. Reportez-vous à la procédure associée dans [Modification de noms d'hôtes et d'adresses IP](#).

- 4 Une fois que les dispositifs sont complètement en ligne avec leur nom de domaine complet d'origine, connectez-vous à chaque nœud IaaS et suivez les étapes suivantes.

- a Ouvrez le fichier suivant dans un éditeur de texte.

```
C:\Program Files (x86)\VMware\VCAC\Management Agent
\VMware.IaaS.Management.Agent.exe.Config
```

- b Modifier chaque nom de domaine complet de endpoint address= du dispositif et leur attribuer le nom de domaine complet d'origine.

Par exemple, à partir de :

```
<endpoint address="https://va1.domain2.local:5480/"
thumbprint="90C55BAEC53E31609EE1614CE4A8336848A8D4CF" />
<endpoint address="https://va2.domain2.local:5480/"
thumbprint="0468BF6EDBC6F2209BE01D0D7FD1094197E324ED" />
```

Au :

```
<endpoint address="https://va1.domain1.local:5480/"
thumbprint="90C55BAEC53E31609EE1614CE4A8336848A8D4CF" />
<endpoint address="https://va2.domain1.local:5480/"
thumbprint="0468BF6EDBC6F2209BE01D0D7FD1094197E324ED" />
```

c Enregistrez et fermez VMware.IaaS.Management.Agent.exe.Config.

- 5 Connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.

<https://vrealize-automation-appliance-FQDN:5480>

- 6 Accédez à **vRA > Messagerie** et cliquez sur **Réinitialiser le cluster RabbitMQ**.
- 7 Une fois la réinitialisation terminée, connectez-vous à chaque interface de gestion de dispositif.
- 8 Accédez à **Cluster**, puis vérifiez que tous les nœuds sont connectés au cluster.

Configurer le groupe de disponibilité AlwaysOn SQL

Vous devez apporter des modifications de configuration si vous définissez le groupe de disponibilité AlwaysOn (AAG) SQL après l'installation de vRealize Automation.

Lorsque vous configurez le groupe AAG SQL après l'installation, suivez les étapes de [Article 2074607 de la base de connaissances VMware](#) pour configurer vRealize Automation avec le nom de domaine complet de l'écouteur AAG en tant qu'hôte SQL Server.

Ajouter des contrôleurs d'interface réseau après l'installation de vRealize Automation

vRealize Automation prend en charge plusieurs contrôleurs d'interface réseau (NIC). Après l'installation, vous pouvez ajouter des cartes réseau au dispositif vRealize Automation ou au serveur Windows IaaS.

Plusieurs cartes réseau peuvent être nécessaires pour certains déploiements vRealize Automation, par exemple :

- Vous souhaitez séparer les réseaux utilisateur et infrastructure.
- Vous avez besoin d'une carte réseau supplémentaire afin que les serveurs IaaS puissent joindre un domaine Active Directory.

Pour plus d'informations sur les multiples scénarios de carte réseau, consultez cette [publication du blog VMware Cloud Management](#).

En présence de trois cartes réseau ou plus, tenez compte des limitations suivantes.

- VIDM a besoin d'accéder à la base de données Postgres et à Active Directory.
- Dans un cluster HA, VIDM a besoin d'accéder à l'URL d'équilibrage de charge.
- Les connexions de VIDM précédentes doivent provenir des deux premières cartes réseau.
- Les cartes réseau venant après la deuxième carte réseau ne doivent pas être utilisées ni reconnues par VIDM.
- Les cartes réseau venant après la deuxième carte réseau ne doivent pas être utilisées pour se connecter à Active Directory.

Utilisez la première ou la seconde carte réseau lors de la configuration d'un annuaire dans vRealize Automation.

Conditions préalables

Installez complètement vRealize Automation dans votre environnement vCenter.

Procédure

- 1 Dans vCenter, ajoutez des cartes réseau à chaque dispositif vRealize Automation.
 - a Cliquez avec le bouton droit sur le dispositif et sélectionnez **Modifier les paramètres**.
 - b Ajoutez des cartes réseau VMXNETn.
 - c S'il est sous tension, redémarrez le dispositif.
- 2 Connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.
 https://vrealize-automation-appliance-FQDN:5480
- 3 Sélectionnez **Réseau**, puis vérifiez que plusieurs cartes réseau sont disponibles.
- 4 Sélectionnez **Adresse** et configurez l'adresse IP des cartes réseau.

Tableau 7-4. Exemple de configuration de carte réseau

Configuration	Valeur
Type d'adresse IPv4	Statique
Adresse IPv4	172.22.0.2
Masque de réseau	255.255.255.0

- 5 Vérifiez que tous les nœuds vRealize Automation peuvent se résoudre mutuellement par nom DNS.
- 6 Vérifiez que tous les nœuds vRealize Automation peuvent accéder à des noms de domaine complets à équilibrage de charge pour les composants vRealize Automation.

- 7 Si vous utilisez Split-Brain DNS, vérifiez que tous les nœuds vRealize Automation et les adresses IP virtuelles ont le même nom de domaine complet dans DNS pour l'adresse IP et l'adresse IP virtuelle (VIP) de chaque nœud.
- 8 Dans vCenter, ajoutez des cartes réseau aux serveurs Windows IaaS.
 - a Cliquez avec le bouton droit sur le serveur IaaS et sélectionnez **Modifier les paramètres**.
 - b Ajoutez des cartes réseau à la machine virtuelle du serveur IaaS.
- 9 Sous Windows, configurez les cartes réseau du serveur IaaS ajoutées et leurs adresses IP. Si nécessaire, consultez la documentation Microsoft.

Étape suivante

(Facultatif) Si vous avez besoin d'itinéraires statiques, consultez [Configurer des routes statiques](#).

Configurer des routes statiques

Lors de l'ajout de cartes réseau à une installation vRealize Automation, si vous avez besoin de routes statiques, vous ouvrez une session d'invite de commandes pour les configurer.

Conditions préalables

Ajoutez plusieurs cartes réseau à des dispositifs vRealize Automation ou à des serveurs Windows IaaS.

Procédure

- 1 Connectez-vous à la ligne de commande du dispositif vRealize Automation en tant qu'utilisateur racine.
- 2 Ouvrez le fichier d'itinéraires dans un éditeur de texte.

```
/etc/sysconfig/network/routes
```

- 3 Recherchez la ligne `default` pour la passerelle par défaut, mais ne la modifiez pas.

Note Dans les cas où il faut changer la passerelle par défaut, utilisez plutôt l'interface de gestion de vRealize Automation.

- 4 Sous la ligne `default`, ajoutez de nouvelles lignes pour les itinéraires statiques. Par exemple :

```
default 10.10.10.1 - -
172.30.30.0 192.168.100.1 255.255.255.0 eth0
192.168.210.0 192.168.230.1 255.255.255.0 eth2
```

- 5 Enregistrez et fermez le fichier d'itinéraires.
- 6 Redémarrez le dispositif.
- 7 Dans les clusters HA, répétez le processus pour chaque dispositif.
- 8 Connectez-vous au serveur Windows IaaS en tant qu'administrateur.

- 9 Ouvrez une invite de commandes en tant qu'administrateur.
- 10 Pour configurer un itinéraire statique, entrez la commande `route -p add`, où `-p` maintient l'itinéraire statique lors des redémarrages successifs. Par exemple :

```
C:\Windows\system32> route -p add 172.30.30.0 mask 255.255.255.0 192.168.100.1 metric 1
OK!
```

Pour plus d'informations sur la configuration des itinéraires statiques dans Windows, consultez la documentation de Microsoft.

Gestion des correctifs accés

Le support technique pour votre installation vRealize Automation peut impliquer un correctif logiciel que vous installez ou supprimez à l'aide de l'interface de gestion de dispositif vRealize Automation.

Pour vous aider à résoudre les problèmes qui peuvent se produire pratiquement en temps réel, des instructions relatives aux correctifs, aux conditions préalables et à l'installation sont disponibles dans la [Base de connaissances VMware](#). Par exemple, l'[article 60310 de la base de connaissances VMware](#) est surveillé et mis à jour avec les dernières informations de correctif vRealize Automation 7.5.

L'interface de correctif ne peut pas appliquer de correctif aux composants vRealize Automation suivants.

- L'agent de gestion
- Agents non vSphere, tel que XenServer, VDI ou Hyper-V

Procédure

- 1 Connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Cliquez sur **vRA > Correctifs**.
- 3 Sous Gestion des correctifs, cliquez sur l'option dont vous avez besoin et suivez les invites.

Option	Description
Nouveau correctif	Installez un nouveau correctif que vous avez téléchargé.
Correctifs installés	Ajoutez le correctif récemment installé aux nœuds de cluster récemment ajoutés.
Retour arrière	Supprimez le correctif le plus récemment installé et restaurez vRealize Automation au niveau de correctif précédent.
Historique	Examinez la liste des correctifs installés et supprimés.

Pour activer ou désactiver la gestion des correctifs, connectez-vous à l'invite de commandes du dispositif vRealize Automation en tant qu'utilisateur racine et entrez l'une des commandes suivantes.

```
/opt/vmware/share/htdocs/service/hotfix/scripts/hotfix.sh enable
/opt/vmware/share/htdocs/service/hotfix/scripts/hotfix.sh disable
```

Configurer l'accès au locataire par défaut

Vous devez octroyer à votre équipe des droits d'accès au locataire par défaut avant qu'elle puisse configurer vRealize Automation.

Le locataire par défaut est automatiquement créé lorsque vous configurez l'assistant d'installation de single sign-on. Vous ne pouvez pas modifier les détails du locataire, par exemple le nom ou le jeton URL, mais vous pouvez créer de nouveaux utilisateurs locaux et nommer des administrateurs de locataire ou IaaS supplémentaires à tout moment.

Procédure

- 1 Connectez-vous à vRealize Automation en tant qu'administrateur du locataire par défaut.
 - a Accédez à l'interface du produit vRealize Automation.
`https://vrealize-automation-FQDN/vcac`
 - b Connectez-vous avec le nom d'utilisateur **administrateur** et le mot de passe que vous avez défini pour cet utilisateur lorsque vous avez configuré SSO.
- 2 Sélectionnez **Administration > Locataires**.
- 3 Cliquez sur le nom du locataire par défaut, **vsphere.local**.
- 4 Cliquez sur l'onglet **Utilisateurs locaux**.
- 5 Créez des comptes d'utilisateurs locaux pour le locataire vRealize Automation par défaut.
 Les utilisateurs locaux sont spécifiques au locataire et peuvent uniquement accéder au locataire dans lequel vous les avez créés.
 - a Cliquez sur l'icône Ajouter (+).
 - b Entrez les détails de l'utilisateur responsable de l'administration de votre infrastructure.
 - c Cliquez sur **Ajouter**.
 - d Recommencez ces étapes pour ajouter un ou plusieurs utilisateurs supplémentaires responsables de la configuration du locataire par défaut.
- 6 Cliquez sur l'onglet **Administrateurs**.

7 Attribuez à vos utilisateurs locaux les rôles d'administrateur de locataires et d'administrateur laaS.

- a Entrez un nom d'utilisateur dans la zone de recherche **Administrateurs de locataire** et appuyez sur Entrée.
- b Entrez un nom d'utilisateur dans la zone de recherche **Administrateurs laaS** et appuyez sur Entrée.

L'administrateur laaS est responsable de la création et de la gestion de vos points de terminaison d'infrastructure dans vRealize Automation. Seul l'administrateur système peut octroyer ce rôle.

8 Cliquez sur **Mise à jour**.

Étape suivante

Fournissez à votre équipe l'URL d'accès et les informations de connexion aux comptes d'utilisateurs que vous avez créés afin qu'ils puissent commencer la configuration de vRealize Automation.

- Vos administrateurs de locataire configurent des paramètres comme l'authentification d'utilisateur, notamment la configuration de Gestion des annuaires pour la haute disponibilité. Reportez-vous à *Configuration de vRealize Automation*.
- Vos administrateurs laaS préparent des ressources externes à des fins de provisionnement. Reportez-vous à *Configuration de vRealize Automation*.
- Si vous avez configuré la création de contenu initial pendant l'installation, votre administrateur de configuration peut demander à l'élément du catalogue Contenu initial de renseigner rapidement une validation technique.

Dépannage de l'installation de vRealize Automation

8

La résolution de problèmes de vRealize Automation fournit des procédures vous permettant de résoudre les problèmes que vous pouvez rencontrer lors de l'installation ou de la configuration de vRealize Automation.

Ce chapitre contient les rubriques suivantes :

- [Emplacement des journaux par défaut](#)
- [Restauration d'une installation qui a échoué](#)
- [Création d'un bundle de support vRealize Automation](#)
- [Dépannage de l'installation générale](#)
- [Dépannage du dispositif vRealize Automation](#)
- [Dépannage des composants IaaS](#)
- [Dépannage des erreurs de connexion](#)

Emplacement des journaux par défaut

Consultez les fichiers journaux système et des produits pour obtenir des informations sur une installation ayant échoué.

Note Pour la collecte de journaux, vous pouvez tirer parti des packs de contenu vRealize Automation et vRealize Orchestrator pour vRealize Log Insight. Les packs de contenu et Log Insight fournissent un résumé consolidé des événements du journal pour les composants de vRealize Suite. Pour en savoir plus, consultez le site [VMware Solution Exchange](#).

Pour consulter la liste des emplacements des journaux la plus récente, reportez-vous à [Article 2141175 de la base de connaissances VMware](#).

Journaux Windows

Utilisez l'emplacement suivant pour trouver les fichiers journaux d'événements Windows.

Journal	Emplacement
Journaux de l'Observateur d'événements Windows	Démarrer > Panneau de configuration > Outil d'administration > Observateur d'événements

Journaux d'installation

Les journaux d'installation se trouvent aux emplacements suivants.

Journal	Emplacement par défaut
Journaux d'installation	C:\Program Files (x86)\vCAC\InstallLogs C:\Program Files (x86)\VMware\vCAC\Server\ConfigTool\Log
Journaux d'installation WAPI	C:\Program Files (x86)\VMware\vCAC\Web API\ConfigTool\Logfilename WapiConfiguration-<XXX>

Journaux IaaS

Les journaux IaaS se trouvent aux emplacements suivants.

Journal	Emplacement par défaut
Journaux de site Web	C:\Program Files (x86)\VMware\vCAC\Server\Website\Logs
Journal de référentiel	C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Web\Logs
Journaux de Manager Service	C:\Program Files (x86)\VMware\vCAC\Server\Logs
Journaux de DEM Orchestrator	C:\Users\<user-name>\AppData\Local\Temp\VMware\vCAC\Distributed Execution Manager\<system-name> DEO \Logs
Journaux d'agents	C:\Users\<user-name>\AppData\Local\Temp\VMware\vCAC\Agents\<agent-name>\logs

Journaux de l'infrastructure vRealize Automation

Les entrées de journaux pour les infrastructures vRealize Automation se trouvent à l'emplacement suivant.

Journal	Emplacement par défaut
Journaux de l'infrastructure	/var/log/vmware

Journaux de provisionnement des composants logiciels

Les journaux de provisionnement des composants logiciels se trouvent à l'emplacement suivant.

Journal	Emplacement par défaut
Journal de démarrage d'agent logiciel	/opt/vmware-appdirector (pour Linux) ou \opt\vmware-appdirector (pour Windows)
Journaux de script de cycle de vie de logiciels	/tmp/taskId (pour Linux) \Users\darwin\AppData\Local\Temp\taskId (pour Windows)

Collection de journaux pour les déploiements distribués

Vous pouvez créer un fichier zip qui regroupe tous les journaux des composants d'un déploiement distribué. .

Restauration d'une installation qui a échoué

En cas d'échec et de restauration d'une installation, l'administrateur système doit vérifier que tous les fichiers requis ont été désinstallés avant de démarrer une autre installation. Certains fichiers doivent être désinstallés manuellement.

Restaurer une installation minimale

Pour désinstaller complètement une installation IaaS vRealize Automation ayant échoué, un administrateur système doit supprimer manuellement certains fichiers et rétablir la base de données.

Procédure

- 1 Si les composants suivants sont présents, désinstallez-les avec le programme de désinstallation de Windows.

- Agents vRealize Automation
- DEM-Worker vRealize Automation
- DEM-Orchestrator vRealize Automation
- Serveur vRealize Automation Server
- WAPI de vRealize Automation

Note Si le message suivant s'affiche, redémarrez la machine et procédez comme suit :
Erreur à l'ouverture du fichier journal d'installation. Vérifiez que
l'emplacement du fichier journal spécifié existe et est inscriptible

Note Si le système Windows a été rétabli ou si vous avez désinstallé IaaS, vous devez exécuter la commande `iisreset` avant de réinstaller l'IaaS de vRealize Automation.

- 2 Rétablissez votre base de données l'état dans laquelle elle se trouvait avant le démarrage de l'installation. La méthode à employer dépend de la méthode d'installation de la base de données originale.
- 3 Dans IIS (Internet Information Services Manager), sélectionnez le site Web par défaut (ou un site personnalisé) et cliquez sur **Liaisons**. Supprimez la liaison https (valeur par défaut 443).
- 4 Vérifiez que le référentiel d'applications, vRealize Automation et le WAPI ont été supprimés et que les pools d'applications RepositoryAppPool, vCACAppPool et WapiAppPool ont été également supprimés.

Résultats

L'installation est complètement supprimée.

Restaurer une installation distribuée

Pour désinstaller complètement une installation IaaS ayant échoué, un administrateur système doit supprimer manuellement certains fichiers et rétablir la base de données.

Procédure

- 1 Si les composants suivants sont présents, désinstallez-les avec le programme de désinstallation de Windows.

- Serveur vRealize Automation
- WAPI de vRealize Automation

Note Si le message suivant s'affiche, redémarrez la machine et procédez comme suit :
 Erreur à l'ouverture du fichier journal d'installation. Vérifiez que
 l'emplacement du fichier journal spécifié existe et est inscriptible.

Note Si le système Windows a été rétabli ou si vous avez désinstallé IaaS, vous devez exécuter la commande `iisreset` avant de réinstaller l'IaaS de vRealize Automation.

- 2 Rétablissez votre base de données à l'état dans laquelle elle se trouvait avant le démarrage de l'installation. La méthode à employer dépend de la méthode d'installation de la base de données originale.
- 3 Dans IIS (Internet Information Services Manager), sélectionnez le site Web par défaut (ou un site personnalisé) et cliquez sur **Liaisons**. Supprimez la liaison https (valeur par défaut 443).
- 4 Vérifiez que le référentiel d'applications, le vCAC et le WAPI ont été supprimés et que les pools d'applications RepositoryAppPool, vCACAppPool et WapiAppPool ont été également supprimés.

Résultats

Tableau 8-1. Restaurer des points d'échec

Point d'échec	Action
Installation de Manager Service	S'il est présent, désinstallez le serveur vCloud Automation Center.
Installation de DEM-Orchestrator	S'il est présent, désinstallez le DEM Orchestrator.
Installation de DEM-Worker	S'il est présent, désinstallez tous les DEM Workers.
Installation d'un agent	S'il est présent, désinstallez tous les agents vRealize Automation.

Création d'un bundle de support vRealize Automation

Vous pouvez créer un bundle de support vRealize Automation à l'aide de l'interface de gestion du dispositif vRealize Automation. Les bundles de support collectent les journaux et vous permettent, ainsi qu'au support technique de VMware, de résoudre les problèmes de vRealize Automation.

Procédure

- 1 Connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.

`https://vrealize-automation-appliance-FQDN:5480`
- 2 Cliquez sur **vRA > Journaux**.
- 3 Cliquez sur **Créer un bundle de support**.
- 4 Cliquez sur **Télécharger** et enregistrez le fichier du bundle de support sur votre système.

Résultats

Les bundles de support incluent des informations sur le dispositif vRealize Automation et les serveurs Windows IaaS. Si vous perdez la connectivité entre le dispositif vRealize Automation et les composants IaaS, le bundle de support ne dispose peut-être pas des journaux de composant IaaS.

Pour afficher les fichiers journaux collectés, décompressez le bundle de support et ouvrez le fichier `Environment.html` dans un navigateur Web. Sans connectivité, les composants IaaS peuvent s'afficher en rouge dans la table Nœuds. Il se peut également que les journaux IaaS soient manquants du fait que le service vRealize Automation Management Agent s'est arrêté sur les serveurs Windows IaaS qui s'affichent en rouge.

Ligne de commande : pour générer un bundle de support à partir de la ligne de commande du dispositif vRealize Automation en tant qu'utilisateur racine, vous pouvez exécuter `vcac-support` ou `vcac-config log-bundle`.

Vous pouvez également exécuter la commande `log-bundle` complète comme indiqué dans l'exemple suivant. Reportez-vous à [vRealize Automation Notions de base sur l'installation depuis la ligne de commande](#) pour obtenir des informations générales sur l'exécution de `vra-command`.

```
# vra-command execute --node cafe.node.497772175.21500 log-bundle --requestor va-1.mycompany.com
```

```
Parent command with id='981e3028-c99b-5c92-1bae-7d2bf5b6aaaa' was created.  
Waiting for all child commands to complete...
```

```
...
```

```
Command execution result:
```

```
Command id: 3d64d122-0af1-28dd-b5a5-d932b78b3678
```

```
  Type: log-bundle
```

```
  Node id: cafe.node.497772175.21500
```

```
  Node host: va-1.mycompany.com
```

```
  Result: The command was successfully executed.
```



```
Result description: {"path": "/opt/vmware/var/support-bundle/log/va-1.mycompany.com_cafe.node.497772175.21500-VA.zip"}
```

Status: COMPLETED

Dépannage de l'installation générale

Les rubriques consacrées au dépannage de dispositifs vRealize Automation proposent des solutions à des problèmes potentiels liés à l'installation que vous pourriez rencontrer en utilisant vRealize Automation.

L'installation des mises à niveau échoue avec une erreur de délai d'attente des équilibrages de charge

Une installation ou une mise à niveau de vRealize Automation pour un déploiement distribué avec un équilibrage de charge échoue et renvoie une erreur de service 503 non disponible.

Problème

L'installation ou la mise à niveau échoue, car le paramètre d'expiration de l'équilibrage de charge n'accorde pas suffisamment de temps pour l'exécution de la tâche.

Cause

Un paramètre de délai d'expiration d'équilibrage de charge insuffisant peut entraîner un échec. Vous pouvez corriger le problème en augmentant le paramètre de délai d'expiration de l'équilibrage de charge à 100 secondes ou plus et en réexécutant la tâche.

Solution

- 1 Augmentez la valeur du délai d'expiration de l'équilibrage de charge à au moins 100 secondes.
- 2 Réexécutez l'installation ou la mise à niveau.

Les heures des serveurs ne sont pas synchronisées

Une installation peut échouer lorsque les serveurs de temps IaaS ne sont pas synchronisés avec le dispositif vRealize Automation.

Problème

Vous ne pouvez pas vous connecter après une installation ou l'installation échoue pendant son exécution.

Cause

Les serveurs de temps de tous les serveurs ne sont peut-être pas synchronisés.

Solution

Synchronisez tous les dispositifs vRealize Automation et serveurs IaaS Windows avec la même source de temps. Ne mélangez pas les sources de temps au sein d'un déploiement vRealize Automation.

- Définissez une source de temps de dispositif vRealize Automation :
 - a Connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.

https://vrealize-automation-appliance-FQDN:5480
 - b Sélectionnez **Admin > Paramètres de l'heure** et définissez la source de synchronisation de l'heure.

Option	Description
Heure de l'hôte	Se synchroniser avec l'hôte ESXi du dispositif vRealize Automation.
Serveur de temps	Se synchroniser avec un serveur NTP (Network Time Protocol) externe. Entrez le nom de domaine complet ou l'adresse IP du serveur NTP.

- Pour les serveurs IaaS Windows, consultez [Activer la synchronisation de l'heure sur le serveur Windows](#).

Des pages blanches peuvent apparaître lors de l'utilisation d'Internet Explorer 9 ou 10 sur Windows 7

Lorsque vous utilisez Internet Explorer 9 ou 10 sur Windows 7 et que le mode de compatibilité est activé, certaines pages restent blanches.

Conditions préalables

Assurez-vous que la barre de menus est affichée. Si vous utilisez Internet Explorer 9 ou 10, appuyez sur Alt pour afficher la barre de menus (ou cliquez avec le bouton droit de la souris sur la barre d'adresse, puis sélectionnez **Barre de menus**).

Problème

Lors de l'utilisation d'Internet Explorer 9 ou 10 sur Windows 7, les pages suivantes restent blanches :

- Infrastructure.
- Dossier locataire par défaut sur la page Orchestrator.
- Configuration de serveur sur la page Orchestrator.

Cause

Le problème peut s'expliquer par le fait que le mode de compatibilité est activé. Vous pouvez désactiver le mode de compatibilité pour Internet Explorer en procédant comme suit.

Solution

- 1 Sélectionnez **Outils > Paramètres d'affichage de compatibilité**.
- 2 Décochez **Afficher les sites intranet en mode de compatibilité**.
- 3 Cliquez sur **Fermer**.

Impossible d'établir une relation de confiance pour le canal sécurisé SSL/TLS

Il se peut que le message suivant s'affiche : « Impossible d'établir une relation de confiance pour le canal sécurisé SSL/TLS lors de la mise à niveau des certificats de sécurité pour vCloud Automation Center. »

Problème

Si un problème de certificat se produit avec vcac-config.exe lors de la mise à niveau d'un certificat de sécurité, le message suivant peut s'afficher :

La connexion sous-jacente a été fermée : impossible d'établir une relation de confiance pour le canal sécurisé SSL/TLS.

Vous pouvez obtenir davantage d'informations sur la cause de ce problème en utilisant la procédure suivante.

Solution

- 1 Ouvrez vcac-config.exe.config dans un éditeur de texte, puis localisez l'adresse du référentiel :

```
<add key="repositoryAddress" value="https://IaaS-address:443/repository/" />
```
- 2 Ouvrez Internet Explorer à l'adresse.
- 3 Parcourez tous les messages d'erreur éventuels concernant des problèmes de confiance de certificat.
- 4 Obtenez un rapport de sécurité dans Internet Explorer, puis utilisez-le pour déterminer pourquoi le certificat n'est pas approuvé.

Solution

Si les problèmes persistent, répétez la procédure en recherchant l'adresse devant être enregistrée, l'adresse du point de terminaison que vous avez utilisé pour vous enregistrer avec vcac-config.exe.

Se connecter au réseau par le biais d'un serveur proxy

Certains sites peuvent se connecter à Internet par le biais d'un serveur proxy.

Conditions préalables

Obtenez de votre administrateur des noms, des numéros de port et des informations d'identification de serveurs proxy.

Problème

Votre déploiement ne peut pas se connecter au réseau Internet ouvert. Par exemple, vous ne pouvez pas accéder à des sites Web, des clouds publics que vous pouvez gérer ou des adresses de fournisseurs à partir desquelles vous pouvez télécharger des logiciels ou des mises à jour.

Cause

Votre site se connecte à Internet par le biais d'un serveur proxy.

Solution

- 1 Ouvrez un navigateur Web et accédez à l'URL de l'interface de gestion du dispositif vRealize Automation.

`https://vrealize-automation-appliance-FQDN:5480`
- 2 Connectez-vous en tant qu'utilisateur racine, puis cliquez sur **Réseau**.
- 3 Entrez le nom de domaine complet ou l'adresse IP, et le numéro de port du serveur proxy de votre site.
- 4 Si votre serveur proxy nécessite des informations d'identification, entrez le nom d'utilisateur et le mot de passe.
- 5 Cliquez sur **Enregistrer les paramètres**.

Étape suivante

La configuration pour l'utilisation d'un serveur proxy peut affecter l'accès de l'utilisateur à VMware Identity Manager. Pour corriger ce problème, reportez-vous à [Le proxy empêche l'utilisateur de VMware Identity Manager de se connecter](#).

Étapes sur la console pour une configuration de contenu initial

Il existe une solution alternative à l'utilisation de l'interface d'installation de vRealize Automation pour créer le compte de l'administrateur de configuration et le contenu initial.

Au lieu d'utiliser l'interface, entrez des commandes de console pour créer l'utilisateur configurationadmin et le contenu initial. Notez que l'interface peut échouer après exécution d'une partie du processus. Il est donc possible que vous n'ayez besoin que de certaines commandes.

Par exemple, vous pouvez inspecter les journaux et l'exécution du workflow vRealize Orchestrator, puis déterminer que la configuration basée sur l'interface a créé l'utilisateur configurationadmin mais pas le contenu initial. Dans ce cas, vous pouvez entrer seulement les deux dernières commandes de consoles pour terminer le processus.

Problème

Lors de la dernière partie de l'installation de vRealize Automation, vous suivez le processus d'entrée d'un nouveau mot de passe, créez le compte utilisateur local configurationadmin et créez le contenu initial. Une erreur se produit et l'interface entre dans un état non récupérable.

Solution

- 1 Connectez-vous à la console du dispositif vRealize Automation en tant qu'utilisateur racine.
- 2 Importez le workflow vRealize Orchestrator en entrant la commande suivante :

```
/usr/sbin/vcac-config -e content-import --workflow /usr/lib/vcac/tools/initial-config/vra-initial-config-bundle-workflow.package --user $SSO_ADMIN_USERNAME --password $SSO_ADMIN_PASSWORD --tenant $TENANT
```

- 3 Exécutez le workflow pour créer l'utilisateur configurationadmin :

```
/usr/bin/python /opt/vmware/share/htdocs/service/wizard/initialcontent/workflowexecutor.py --host $CURRENT_VA_HOSTNAME --username $SSO_ADMIN_USERNAME --password $SSO_ADMIN_PASSWORD --workflowid f2b3064a-75ca-4199-a824-1958d9c1efed --configurationAdminPassword $CONFIGURATIONADMIN_PASSWORD --tenant $TENANT
```

- 4 Pour importer le Blueprint ASD, entrez la commande suivante :

```
/usr/sbin/vcac-config -e content-import --blueprint /usr/lib/vcac/tools/initial-config/vra-initial-config-bundle-asd.zip --user $CONFIGURATIONADMIN_USERNAME --password $CONFIGURATIONADMIN_PASSWORD --tenant $TENANT
```

- 5 Exécutez le workflow pour configurer le contenu initial :

```
/usr/bin/python /opt/vmware/share/htdocs/service/wizard/initialcontent/workflowexecutor.py --host $CURRENT_VA_HOSTNAME --username $SSO_ADMIN_USERNAME --password $SSO_ADMIN_PASSWORD --workflowid ef00fce2-80ef-4b48-96b5-fdee36981770 --configurationAdminPassword $CONFIGURATIONADMIN_PASSWORD
```

Impossible de rétrograder les licences de vRealize Automation

Une erreur se produit lorsque vous soumettez la clé de licence d'une édition inférieure du produit.

Problème

Le message suivant s'affiche lors de l'utilisation de la page de gestion des licences de l'interface d'administration de vRealize Automation pour envoyer la clé à une édition de produit inférieure à l'édition actuelle. Par exemple, vous utilisez par une licence d'entreprise et essayez d'entrer une licence avancée.

```
Unable to downgrade existing license edition
```

Cause

Cette version de vRealize Automation ne prend pas en charge la rétrogradation de licences. Vous pouvez uniquement ajouter des licences d'une édition équivalente ou supérieure.

Solution

Pour passer à une édition inférieure, réinstallez vRealize Automation.

Dépannage du dispositif vRealize Automation

Les articles relatifs au dépannage de dispositifs vRealize Automation proposent des solutions aux possibles problèmes liés à l'installation que vous pouvez rencontrer lors de l'utilisation des dispositifs vRealize Automation.

Le téléchargement des programmes d'installation échoue

Le téléchargement des programmes d'installation échouent à partir du dispositif vRealize Automation.

Problème

Les programmes d'installation ne se téléchargent pas lors de l'exécution de `setup__vrealize-automation-appliance-FQDN@5480.exe`.

Cause

- Problèmes de connectivité réseau lors de la connexion à la machine du dispositif vRealize Automation.
- Impossible de se connecter à la machine du dispositif vRealize Automation, car la machine est inaccessible ou ne répond pas avant l'expiration du délai de connexion.

Solution

- 1 Vérifiez que vous pouvez vous connecter à l'URL vRealize Automation dans un navigateur Web.
`https://vrealize-automation-appliance-FQDN`
- 2 Consultez les autres rubriques de dépannage du dispositif vRealize Automation.
- 3 Téléchargez le fichier de configuration et reconnectez-vous au dispositif vRealize Automation.

Le fichier Encryption.key comporte des autorisations incorrectes

Une erreur système peut survenir si des autorisations incorrectes sont attribuées au fichier Encryption.key pour un dispositif virtuel.

Conditions préalables

Connectez-vous au dispositif virtuel qui affiche l'erreur.

Note Si vos dispositifs virtuels sont exécutés sous un équilibrage de charge, vous devez vérifier chacun d'entre eux.

Problème

Vous vous connectez à dispositif vRealize Automation et la page Locataires s'affiche. Une fois que la page a commencé à se charger, le message Erreur système s'affiche.

Cause

Le fichier Encryption.key comporte des autorisations incorrectes ou le niveau de groupe ou d'utilisateur propriétaire est attribué de manière incorrecte.

Solution

- 1 Affichez le fichier journal `/var/log/vcac/catalina.out` et recherchez le message `Cannot write to /etc/vcac/Encryption.key`.
- 2 Accédez au répertoire `/etc/vcac/` et vérifiez les autorisations et la propriété pour le fichier `Encryption.key`. Vous devez voir une ligne similaire à la suivante :

```
-rw----- 1 vcac vcac 48 Dec 4 06:48 encryption.key
```

Read and write permission is required and the owner and group for the file must be `vcac`.

- 3 Si le résultat que vous voyez est différent, modifiez les autorisations et la propriété du fichier si nécessaire.

Étape suivante

Connectez-vous à la page Locataire pour vérifier que vous pouvez vous connecter sans erreur.

Échec du démarrage d'Identity Manager pour la gestion des annuaires après le redémarrage de Horizon-Workspace

Dans un environnement vRealize Automation à haute disponibilité, le démarrage d'Identity Manager peut échouer après le redémarrage du service horizon-workspace.

Problème

Le service horizon-workspace ne peut pas démarrer à cause d'une erreur similaire à celle qui suit :

```
Error creating bean with name
'liquibase' defined in class path resource [spring/datastore-wireup.xml]:
Invocation of init method failed; nested exception is
liquibase.exception.LockException: Could not acquire change log lock. Currently
locked by fe80:0:0:0:250:56ff:fea8:7d0c%eth0
(fe80:0:0:0:250:56ff:fea8:7d0c%eth0) since 10/29/15
```

Cause

Identity Manager peut entraîner un échec au démarrage dans un environnement à haute disponibilité à cause de problèmes liés à l'utilitaire de gestion des données de liquibase utilisées par vRealize Automation.

Solution

- 1 Connectez-vous en tant qu'utilisateur racine à une session de console sur le dispositif vRealize Automation.
- 2 Arrêtez le service horizon-workspace en entrant la commande suivante.
`#service horizon-workspace stop`
- 3 Ouvrez le shell Postgres en tant que super utilisateur.
`su postgres`
- 4 Accédez au répertoire bin correct.
`cd /opt/vmware/vpostgres/current/bin`
- 5 Connectez-vous à la base de données.
`psql vcac`
- 6 À partir de `saas.databasechangelock`, exécutez la requête SQL suivante.
`select * from databasechangelock;`
Si la sortie affiche la valeur « t » pour true, le verrou doit être désactivé manuellement.
- 7 Si vous désactivez manuellement le verrou, exécutez la requête SQL suivante.
`update saas.databasechangelock set locked=FALSE, lockgranted=NULL, lockedby=NULL where id=1;`
- 8 À partir de `saas.databasechangelock`, exécutez la requête SQL suivante.
`select * from databasechangelock;`
La sortie devrait afficher une valeur de « f » pour false, cela signifie qu'il est déverrouillé.

- 9 Quittez la base de données vcac Postgres.

```
vcac=# \q
```

- 10 Fermez le shell Postgres.

```
exit
```

- 11 Démarrez le service horizon-workspace.

```
#service horizon-workspace start
```

Attributions de rôles de dispositifs incorrectes après basculement

Après un basculement, les nœuds du dispositif vRealize Automation master et de réplica risquent de ne pas disposer de la bonne attribution de rôles, ce qui affecte tous les services nécessitant un accès en écriture à la base de données.

Problème

Dans un cluster à haute disponibilité de dispositifs vRealize Automation, vous arrêtez le nœud master de la base de données ou le rendez inaccessible. Vous utilisez l'interface de gestion sur un autre nœud pour promouvoir celui-ci au rang de nouveau nœud master, ce qui restaure l'accès en écriture à la base de données vRealize Automation.

Ensuite, vous remettez en ligne l'ancien nœud master, mais l'onglet Cluster dans l'interface de gestion indique toujours que le nœud est le nœud master même s'il ne l'est plus. Les tentatives d'utilisation d'une interface de gestion de nœuds pour résoudre le problème en promouvant officiellement l'ancien nœud au rang de nœud master échouent.

Solution

Lors d'un basculement, suivez ces directives pour configurer les anciens et nouveaux nœuds master.

- Avant de promouvoir un autre nœud au rang de nœud master, retirez le nœud master précédent du pool d'équilibrage de charge des nœuds de dispositifs vRealize Automation.
- Pour que vRealize Automation remplace un ancien nœud master dans le cluster, laissez l'ancienne machine venir en ligne. Ouvrez ensuite l'interface de gestion du nouveau nœud master. Recherchez l'ancien nœud signalé comme `invalid` dans l'onglet Cluster, puis cliquez sur son bouton **Réinitialiser**.

Après la réinitialisation, vous pouvez restaurer l'ancien nœud dans le pool d'équilibrage de charge des nœuds de dispositifs vRealize Automation.

- Pour remettre un ancien nœud master dans le cluster, mettez en ligne la machine, puis joignez-la au cluster comme s'il s'agissait d'un nouveau nœud. Lors de la jonction, désignez le nœud récemment promu comme nœud principal.

Après la jonction, vous pouvez restaurer l'ancien nœud dans le pool d'équilibrage de charge des nœuds de dispositifs vRealize Automation.

- Tant que vous n'avez pas réinitialisé ou remis correctement dans le cluster un ancien nœud master, n'utilisez pas son interface de gestion pour les opérations de gestion de clusters, même si le nœud est de nouveau en ligne.
- Après la réinitialisation ou la nouvelle jonction, vous pouvez promouvoir de nouveau l'ancien nœud au rang de nœud master.

Pannes après la promotion de nœuds de réplica et master

Un incident d'espace disque, lié à la promotion de nœuds de base de données de dispositif vRealize Automation de réplica et master, peut provoquer des problèmes de provisionnement.

Problème

Le nœud master n'a plus d'espace disque. Vous vous connectez à sa page de base de données d'interface de gestion, et promouvez un nœud de réplica disposant de suffisamment d'espace pour devenir le nouveau nœud master. La promotion semble réussir lorsque vous actualisez la page d'interface de gestion, même si un message d'erreur s'affiche.

Plus tard, sur le nœud qui était l'ancien nœud master, vous libérez l'espace disque. Cependant, après la repromotion du nœud au rang de master, les opérations de provisionnement échouent et restent bloquées à l'état IN_PROGRESS.

Cause

vRealize Automation ne peut pas correctement mettre à jour l'ancienne configuration de nœud master en présence du problème d'insuffisance d'espace.

Solution

Si l'interface de gestion affiche des erreurs pendant la promotion, excluez temporairement le nœud de l'équilibrage de charge. Corrigez le problème du nœud, en ajoutant par exemple un disque, avant de le réinclure dans l'équilibrage de charge. Ensuite, actualisez la page de base de données de l'interface de gestion et vérifiez que les nœuds appropriés sont les nœuds master et de réplica.

Enregistrements des services composants vRealize Automation incorrects

L'interface de gestion du dispositif vRealize Automation peut vous aider à résoudre des problèmes d'enregistrement avec les services de composants vRealize Automation.

Problème

Dans des conditions normales de fonctionnement, tous les services composants vRealize Automation doit être uniques et dans un état ENREGISTRÉ. Tout autre ensemble de conditions peut entraîner un comportement imprévisible de vRealize Automation.

Cause

Les exemples de problèmes suivants peuvent se produire avec des composants services vRealize Automation.

- Un service est devenu inactif.
- Les paramètres du serveur ont placé le service dans un état autre qu'ENREGISTRÉ.
- Une dépendance sur un autre service a placé le service dans un état autre qu'ENREGISTRÉ.
- Le service SQL peut ne pas être en cours d'exécution.

Solution

Réenregistrez les services de composants qui semblent présenter des problèmes.

- 1 Prenez un snapshot du dispositif vRealize Automation.

Il se peut que vous deviez rétablir le snapshot si vous essayez de différentes modifications de service et que le dispositif finit dans un état imprévisible.

- 2 Connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.

`https://vrealize-automation-appliance-FQDN:5480`

- 3 Cliquez sur **Services**.

- 4 Dans la liste de services, recherchez un service qui n'est pas dans l'état approprié ou présente d'autres problèmes.

- 5 Si un service défectueux est `iaas-service`, accédez à l'étape suivante.

Sinon, pour que vRealize Automation enregistre de nouveau le service, connectez-vous à une session de console sur le dispositif vRealize Automation en tant qu'utilisateur racine, puis redémarrez vRealize Automation en entrant la commande suivante.

```
service vcac-server restart
```

Si des services sont associés à l'instance intégrée de vRealize Orchestrator, entrez la commande supplémentaire suivante.

```
service vco-restart restart
```

- 6 Si un service défectueux est `iaas-service`, procédez comme suit pour l'enregistrer de nouveau.

- a N'annulez pas l'enregistrement du service.
- b Sur le serveur Web IaaS principal, connectez-vous avec un compte disposant de droits d'administrateur.
- c Ouvrez une invite de commande en tant qu'administrateur.
- d Exécutez la commande suivante.

```
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterSolutionUser -url https://appliance-or-load-balancer-IP-or-FQDN/ -t
vsphere.local -cu administrator -cp password -f "C:\Program Files (x86)\VMware\vCAC
\Server\Model Manager Data\Cafe\Vcac-Config.data" -v
```

Le mot de passe est le mot de passe administrator@vsphere.local.

- e Exécutez une commande pour mettre à jour les informations d'enregistrement dans la base de données IaaS.

SQL Server avec l'authentification Windows :

```
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
MoveRegistrationDataToDb -s IaaS-SQL-server-IP-or-FQDN -d SQL-database-name -f
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.data" -v
```

SQL Server avec l'authentification SQL native :

```
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
MoveRegistrationDataToDb -s SQL-server-IP-or-FQDN -d SQL-database-name -su SQL-user -
sp SQL-user-password -f "C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data
\Cafe\Vcac-Config.data" -v
```

Pour trouver le nom du serveur ou de la base de données, examinez le fichier suivant dans un éditeur de texte et recherchez repository. Les valeurs Source de données et Catalogue initial contiennent respectivement l'adresse du serveur et le nom de la base de données.

C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Web\Web.config

L'utilisateur SQL doit disposer de privilèges DBO sur la base de données.

- f Enregistrez les points de terminaison en exécutant les commandes suivantes :

```
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN /vcac
--Endpoint ui -v
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN /WAPI
--Endpoint wapi -v
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN /
repository --Endpoint repo -v
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN /
WAPI/api/status --Endpoint status -v
```

- g Enregistrez les éléments du catalogue en exécutant la commande suivante :

```
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterCatalogTypesAsync -v
```

- h Redémarrez IIS.

```
iisreset
```

i Connectez-vous à l'hôte principal de IaaS Manager Service.

j Redémarrez le service Windows vRealize Automation.

```
VMware vCloud Automation Center Service
```

- 7 Pour réenregistrer des services associés à un système externe, par exemple une instance externe de vRealize Orchestrator, connectez-vous au système externe et redémarrez-y les services.

La carte réseau supplémentaire provoque des erreurs d'interface de gestion

Après avoir ajouté une deuxième carte d'interface réseau à un dispositif vRealize Automation, certaines pages de l'interface de gestion vRealize Automation échouent à se charger correctement.

Problème

Vous ajoutez une deuxième carte réseau à l'aide de vCenter et les pages suivantes de l'interface de gestion vRealize Automation affichent des erreurs au lieu de se charger.

- La page **État > du réseau** affiche une erreur relative à un script qui ne répond pas.
- La page **Adresse > du réseau** affiche une erreur relative à l'échec de la lecture des informations de l'interface réseau.

Cause

Depuis la version 7.3, le dispositif vRealize Automation peut prendre en charge deux cartes réseau. Toutefois, le modèle d'ingénierie sur lequel repose le dispositif empêche l'interface de gestion de fonctionner correctement tant que vous n'appliquez pas la solution.

Solution

Après avoir ajouté une carte réseau supplémentaire, redémarrez le dispositif vRealize Automation.

Impossible de promouvoir un dispositif virtuel secondaire au rang de dispositif master

Dans vRealize Automation, une faible capacité de mémoire de dispositif virtuel peut empêcher les promotions de dispositif virtuel dans le cluster.

Problème

Le nœud master n'a presque plus de mémoire. Vous vous connectez à sa page de base de données d'interface de gestion et essayez de promouvoir un nœud secondaire au rang de nouveau nœud master. L'erreur suivante se produit.

```
Fail to execute on Node node-name, host is master-FQDN
because of: Could not read remote lock command result for node: node-name
on address: master-FQDN, reason is: 500 Internal Server Error
```

Cause

La promotion ne réussit que lorsque tous les nœuds peuvent confirmer la reconfiguration de cette promotion. La faible capacité mémoire empêche l'ancien nœud master de confirmer, même si tous les nœuds sont accessibles.

Solution

Mettez hors tension le nœud master disposant d'une mémoire insuffisante. Connectez-vous à la page de base de données de l'interface de gestion du nœud secondaire, puis procédez à la promotion de ce dernier.

La durée de rétention du journal de synchronisation Active Directory est trop courte

Dans vRealize Automation, les journaux de synchronisation Active Directory ne remontent que de quelques jours.

Problème

Après deux jours, les journaux de synchronisation Active Directory disparaissent de l'interface de gestion. Les dossiers des journaux disparaissent également à partir du répertoire du dispositif vRealize Automation suivant.

```
/db/elasticsearch/horizon/nodes/0/indices
```

Cause

Pour économiser de l'espace, vRealize Automation définit la durée de rétention maximale pour les journaux de la synchronisation Active Directory à trois jours.

Solution

- 1 Connectez-vous à une session de console sur le dispositif vRealize Automation en tant qu'utilisateur racine.
- 2 Ouvrez le fichier suivant dans un éditeur de texte.
`/usr/local/horizon/conf/runtime-config.properties`
- 3 Augmentez la propriété `analytics.maxQueryDays`.
- 4 Enregistrez et fermez `runtime-config.properties`.

5 Redémarrez le Gestionnaire d'identité et les services de recherche élastique.

```
service horizon-workspace restart
service elasticsearch restart
```

RabbitMQ ne parvient pas à résoudre les noms d'hôte

RabbitMQ utilise des noms d'hôte courts pour les dispositifs vRealize Automation par défaut, ce qui risque d'empêcher les nœuds de s'identifier entre eux.

Problème

Vous tentez de joindre un autre dispositif vRealize Automation au cluster et une erreur semblable à l'erreur suivante se produit.

```
Clustering node 'rabbit@sc2-rdops-vm01-dhcp-62-2' with rabbit@company ...
Error: unable to connect to nodes [rabbit@company]: nodedown

DIAGNOSTICS
=====

attempted to contact: [rabbit@company]

rabbit@company:
* unable to connect to epmd (port 4369) on company: nxdomain (non-existing domain)

current node details:
- node name: 'rabbitmq-cli-11@sc2-rdops-vm01-dhcp-62-2'
- home dir: /var/lib/rabbitmq
- cookie hash: 4+kP1tKnxGYaGjrPL2C8bQ==

[2017-09-01 14:58:04] [root] [INFO] RabbitMQ join failed with exit code: 69, see RabbitMQ logs for
details.
```

Cause

Votre configuration réseau ne permet pas aux dispositifs vRealize Automation de s'identifier entre eux via un nom d'hôte court.

Solution

- 1 Pour tous les dispositifs vRealize Automation du déploiement, connectez-vous en tant qu'utilisateur racine dans une session de console.

- 2 Arrêtez le service RabbitMQ.

```
service rabbitmq-server stop
```

- 3 Ouvrez le fichier suivant dans un éditeur de texte.

```
/etc/rabbitmq/rabbitmq-env.conf
```

- 4 Définissez la propriété suivante sur true.

```
USE_LONGNAME=true
```

- 5 Enregistrez et fermez `rabbitmq-env.conf`.

- 6 Réinitialisez RabbitMQ.

```
vcac-vami rabbitmq-cluster-config reset-rabbitmq-node
```

- 7 Sur un seul nœud de dispositif vRealize Automation, exécutez le script suivant.

```
vcac-config cluster-config-ping-nodes --services rabbitmq-server
```

- 8 Sur tous les nœuds, vérifiez que le service RabbitMQ est démarré.

```
vcac-vami rabbitmq-cluster-config get-rabbitmq-status
```

Dépannage des composants IaaS

Les rubriques consacrées au dépannage de composants IaaS vRealize Automation proposent des solutions à des problèmes potentiels liés à l'installation que vous pourriez rencontrer en utilisant vRealize Automation.

Les connexions du coordinateur de transaction distribué sont refusées

Les paramètres d'appel de procédure distante (RPC, Remote Procedure Call) Microsoft peuvent affecter le coordinateur de transactions distribuées (DTC, Distributed Transaction Coordinator) dans vRealize Automation.

Problème

Des erreurs se produisent, indiquant que les connexions DTC entre les serveurs Windows IaaS ou le serveur de base de données SQL vRealize Automation sont refusées.

Cause

Un paramètre de connexion RPC limite l'accès et doit être désactivé.

Solution

Sur tous les serveurs Windows IaaS et sur le serveur de base de données SQL vRealize Automation, supprimez la clé de registre suivante ou définissez-la sur zéro.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\RPC\RestrictRemoteClients
```

Le programme de correction des conditions préalables ne peut pas installer les fonctionnalités .NET

L'option de **correction** du programme de vérification des conditions préalables de vRealize Automation échoue et affiche des messages indiquant que la source d'installation de .NET 3.5.1 est introuvable.

Problème

Le programme de vérification des conditions préalables doit vérifier que .NET 3.5.1 est installé afin de satisfaire aux conditions requises des systèmes Windows Server 2008 R2 avec IIS 7.5 et des systèmes Windows Server 2012 R2 avec IIS 8.

Cause

Pour Windows Server 2012 R2, l'impossibilité de se connecter à Internet peut empêcher l'installation automatique de .NET. Certaines mises à jour de Windows 2012 R2 peuvent également empêcher l'installation. Le problème survient car la version de Windows ne dispose pas d'une copie locale de la source d'installation de .NET Framework 3.5.

Solution

Fournissez manuellement une source d'installation pour .NET Framework 3.5.

- 1 Sur l'hôte Windows, montez une image ISO du support d'installation de Windows Server 2012 R2.
- 2 Dans le gestionnaire de serveur, activez .NET Framework 3.5 à l'aide de l'assistant Ajouter des rôles et des fonctionnalités.
- 3 Pendant l'exécution de l'assistant, accédez au chemin d'installation de .NET Framework 3.5 sur le support ISO.
- 4 Après l'ajout de .NET Framework 3.5, exécutez à nouveau le programme de vérification des conditions préalables de vRealize Automation.

Validation des certificats de serveur pour IaaS

Vous pouvez utiliser la commande `vcac-Config.exe` pour vérifier qu'un serveur IaaS accepte le dispositif vRealize Automation et les certificats du dispositif SSO.

Problème

Des erreurs d'autorisation s'affichent lorsque vous utilisez des fonctionnalités IaaS.

Cause

Des erreurs d'autorisation peuvent se produire lorsque IaaS ne reconnaît pas les certificats de sécurité d'autres composants.

Solution

- 1 Ouvrez une invite de commande en tant qu'administrateur et accédez au répertoire Cafe à l'adresse `vra-installation-dir\Server\Model Manager Data\Cafe`, en général `C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe`.

2 Tapez une commande sous la forme de

Vcac-Config.exe CheckServerCertificates -d [vra-database] -s [vRA SQL server] -v.
Les paramètres facultatifs sont `-su [SQL user name]` et `-sp [password]`.

Si la commande s'exécute avec succès, le message suivant s'affiche :

```
Certificates validated successfully.  
Command succeeded.
```

Si la commande échoue, un message d'erreur détaillé s'affiche.

Note Cette commande est uniquement disponible sur le nœud du composant Model Manager Data.

Erreur d'informations d'identification lors de l'exécution du programme d'installation d'IaaS

Lorsque vous installez des composants IaaS, vous recevez un message d'erreur au moment de saisir vos informations d'identification de dispositif virtuel.

Problème

Après avoir fourni les informations d'identification au programme d'installation d'IaaS, un message d'erreur `org.xml.sax.SAXParseException` s'affiche.

Cause

Vous avez utilisé des informations d'identification incorrectes ou un format d'informations d'identification incorrect.

Solution

- ◆ Vérifiez que vous utilisez les valeurs de locataire et de nom d'utilisateur corrects.

Par exemple, le locataire SSO par défaut utilise comme nom de domaine `vsphere.local` et non `administrator@vsphere.local`.

Un avertissement d'enregistrement des paramètres s'affiche lors de l'installation d'IaaS

Un message s'affiche lors de l'installation d'IaaS. `Warning: Could not save settings to the virtual appliance during IaaS installation.`

Problème

Un message d'erreur inapproprié indiquant que les paramètres utilisateur n'ont pas été enregistrés s'affiche lors de l'installation d'IaaS.

Cause

Des problèmes de communication ou de réseau peuvent entraîner l'affichage erroné de ce message.

Solution

Ignorez ce message d'erreur et poursuivez l'installation. Ce message ne devrait pas l'échec de la configuration.

Échec de l'installation du serveur de site Web et des Distributed Execution Managers

Votre installation du serveur de site Web et des DEM d'infrastructure du dispositif vRealize Automation ne peut pas se poursuivre si le mot de passe de votre compte de service IaaS contient des guillemets.

Problème

Un message s'affiche vous informant que l'installation des DEM distribués et du serveur de site Web du dispositif vRealize Automation a échoué en raison de paramètres msixexec non valides.

Cause

Le compte de service IaaS utilise un guillemet.

Solution

- 1 Vérifiez que le mot de passe de votre compte de service IaaS n'inclut pas de guillemets.
- 2 Si c'est le cas, créez un nouveau mot de passe.
- 3 Redémarrez l'installation.

L'authentification IaaS échoue lors de l'installation d'IaaS Web et de Model Management

Lors de l'exécution de l'outil de vérification des conditions préalables, un message indiquant que le contrôle de l'authentification IIS a échoué s'affiche.

Problème

Le message vous indique que l'authentification n'est pas activée, mais la case à cocher Authentification IIS est sélectionnée.

Solution

- 1 Décochez la case Authentification Windows.
- 2 Cliquez sur **Enregistrer**.
- 3 Cochez la case Authentification Windows.
- 4 Cliquez sur **Enregistrer**.
- 5 Réexécutez l'outil de vérification des conditions préalables.

L'installation des données Model Manager et des composants Web a échoué

Votre installation de vRealize Automation peut échouer si le programme d'installation d'IaaS n'est pas en mesure d'enregistrer le composant Model Manager Data et le composant Web.

Problème

Votre installation échoue et renvoie le message d'erreur suivant :

Le programme d'installation d'IaaS n'a pas pu enregistrer les composants Model Manager Data et Web.

Cause

L'échec peut avoir différentes causes.

- Problèmes de connectivité au dispositif vRealize Automation ou entre les dispositifs. Une tentative de connexion échoue en raison d'une absence de réponse ou de l'impossibilité d'établir une connexion.
- Problèmes de certificat approuvé dans IaaS lors de l'utilisation d'une configuration distribuée.
- Incompatibilité de nom de certificat dans une configuration distribuée.
- Le certificat peut être non valide ou il peut exister une erreur dans la chaîne de certificat.
- Le service du référentiel échoue à démarrer.
- Configuration incorrecte de l'équilibrage de charge dans un environnement distribué.

Solution

◆ Connectivité

Vérifiez que vous pouvez vous connecter à l'URL vRealize Automation dans un navigateur Web.

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

◆ Problèmes de certificat approuvé

- Dans IaaS, ouvrez Microsoft Management Console avec la commande `mmc.exe` et vérifiez que le certificat utilisé dans l'installation a été ajouté au magasin de certificats racines de confiance dans la machine.
- Dans un navigateur Web, vérifiez l'état du service MetaModel et assurez-vous qu'aucune erreur de certificat ne s'affiche :

`https://FQDN-or-IP/repository/data/MetaModel.svc`

◆ Incompatibilité de nom de certificat

Cette erreur peut se produire lorsque le certificat est émis à un nom en particulier et qu'un nom ou une adresse IP différente est utilisée. Vous pouvez supprimer l'erreur d'incompatibilité de nom de certificat au cours de l'installation en sélectionnant **Supprimer les incompatibilités de certificat**.

Vous pouvez utiliser également l'option Supprimer les incompatibilités de certificat pour ignorer les erreurs de correspondance de liste à distance de révocation de certificat.

◆ Certificat non valide

Ouvrez la console de gestion Microsoft avec la commande `mmc.exe`. Vérifiez que le certificat n'a pas expiré et que l'état est correct. Procédez ainsi avec tous les certificats de la chaîne de certificats. Vous pouvez avoir à importer d'autres certificats de la chaîne dans le magasin de certificats racine approuvés lors de l'utilisation d'une hiérarchie de certificats.

◆ Service de référentiel

Utilisez les actions suivantes pour vérifier l'état du service du référentiel.

- Dans un navigateur Web, vérifiez l'état du service MetaModel :
`https://FQDN-or-IP/repository/data/MetaModel.svc`
- Vérifiez le fichier `Repository.log` pour consulter les erreurs.
- Réinitialisez l'IIS (`iisreset`) si vous rencontrez des problèmes avec les applications hébergées sur le site Web (Référentiel, vRealize Automation ou WAPI).
- Vérifiez que le site Web se connecte à `%SystemDrive%\inetpub\logs\LogFiles` pour obtenir des informations supplémentaires sur la connexion.
- Vérifiez que l'outil de vérification des conditions préalables s'exécute correctement lors de la vérification des conditions requises.
- Dans Windows 2012, vérifiez que WCF Services sous .NET Framework est installé et que l'activation HTTP est installée.

Les serveurs Windows IaaS ne prennent pas en charge la norme FIPS

Une installation ne peut pas réussir lorsque la norme Information Processing Standard (FIPS) est activée.

Problème

L'installation échoue et renvoie l'erreur suivante pendant l'installation du composant Web IaaS.

Cette implémentation ne fait pas partie des algorithmes de chiffrement validés Windows Platform FIPS.

Cause

vRealize Automation IaaS est basé sur Microsoft Windows Communication Foundation (WCF) qui ne prend pas en charge la norme FIPS.

Solution

Sur le serveur Windows IaaS, désactivez la stratégie FIPS.

- 1 Accédez à **Démarrer > Panneau de configuration > Outils d'administration > Stratégie de sécurité locale**.
- 2 Dans la boîte de dialogue Stratégie de groupe, sous **Stratégies locales**, sélectionnez **Options de sécurité**.
- 3 Trouvez et désactivez l'entrée suivante.
Cryptographie système : utilisez des algorithmes compatibles FIPS pour le cryptage, le hachage et la signature.

L'ajout d'un point de terminaison XaaS génère une erreur interne

Lorsque vous tentez de créer un point de terminaison XaaS, un message d'erreur interne apparaît.

Problème

La création d'un point de terminaison échoue avec le message d'erreur interne suivant : Une erreur interne s'est produite. Si ce problème persiste, contactez votre administrateur système. Lorsque vous contactez votre administrateur système, utilisez la référence `c0DD0C01`. Les codes de référence sont générés de manière aléatoire et ne sont pas liés à un message d'erreur en particulier.

Solution

- 1 Ouvrez le fichier journal du dispositif vRealize Automation.
`/var/log/vcac/catalina.out`
- 2 Localisez le code de référence dans le message d'erreur.
Par exemple, `c0DD0C01`.
- 3 Recherchez le code de référence dans le fichier journal pour localiser l'entrée associée.
- 4 Passez en revue les entrées qui apparaissent au-dessus et en dessous de l'entrée associée pour résoudre le problème.

L'entrée de journal associé n'appelle pas spécifiquement la source du problème.

Échec de la désinstallation de l'agent proxy

La suppression d'un agent proxy peut échouer si la journalisation du programme d'installation de Windows est activée.

Problème

Lorsque vous essayez de désinstaller un agent proxy dans le Panneau de configuration Windows, l'opération échoue et l'erreur suivante s'affiche :

```
Error opening installation log file. Verify that the
specified log file location exists and is writable
```

Cause

Cela peut se produire si la journalisation du programme d'installation de Windows est activée, mais le moteur du programme d'installation de Windows ne peut pas écrire correctement sur le fichier journal de désinstallation. Pour plus d'informations, reportez-vous à [Article 2564571 de la base de connaissances Microsoft](#).

Solution

- 1 Redémarrez votre machine ou explorer.exe dans le Gestionnaire de tâches.
- 2 Désinstallez l'agent.

Les demandes de machine échouent lorsque les transactions à distance sont désactivées

Les demandes de machines échouent lorsque les transactions distantes du Coordinateur de transactions distribuées (DTC, Distributed Transaction Coordinator) de Microsoft sont désactivées sur des machines serveurs Windows.

Problème

Si vous provisionnez une machine alors que les transactions distantes sont désactivées sur le portail Model Manager ou le serveur SQL Server, la demande n'aboutit pas. La collecte de données échoue et la demande de la machine reste à l'état de workflows de clone.

Cause

Les transactions distantes DTC sont désactivées dans l'instance SQL IaaS utilisée par le système vRealize Automation.

Solution

- 1 Lancez Windows Server Manager pour activer DTC sur tous les serveurs vRealize et serveurs SQL associés.

Dans Windows 7, accédez à **Démarrer > Outils d'administration > Services composants**.

Note Vérifiez que tous les serveurs Windows disposent de SID uniques pour la configuration de MSDTC.

- 2 Ouvrez tous les nœuds pour rechercher le DTC local ou le DTC en cluster si vous utilisez un système en cluster.
Accédez à **Services composants > Ordinateurs > Mon ordinateur > Coordinateur de transaction distribué**.
- 3 Cliquez avec le bouton droit sur le DTC local ou en cluster DTC et sélectionnez **Propriétés**.
- 4 Cliquez sur l'onglet **Sécurité**.
- 5 Sélectionnez l'option **Accès DTC réseau**.
- 6 Sélectionnez les options **Autoriser le client distant** et **Autoriser l'administration à distance**.
- 7 Sélectionnez les options **Autoriser l'accès entrant** et **Autoriser l'accès sortant**.
- 8 Entrez ou sélectionnez NT AUTHORITY\Network Service dans le champ **Compte** du Compte d'ouverture de session DTC.
- 9 Cliquez sur **OK**.
- 10 Supprimez les machines bloquées à l'état Workflow de clone.
 - a Connectez-vous à l'interface du produit vRealize Automation.
`https://vrealize-automation-appliance-FQDN/vcac/org/tenant-name`
 - b Accédez à **Infrastructure > Machines gérées**.
 - c Cliquez avec le bouton droit sur la machine cible.
 - d Sélectionnez **Supprimer** pour supprimer la machine.

Erreur dans la communication de Manager Service

Les serveurs IaaS clonés à partir d'un modèle dans lequel DTC a déjà été installé contiennent des identifiants dupliqués pour DTC, ce qui empêche la communication entre les nœuds.

Problème

Le service de gestion IaaS échoue et affiche l'erreur suivante dans le journal de Manager Service.

```
La communication avec le gestionnaire de transaction sous-jacent a échoué. --->
System.Runtime.InteropServices.COMException : le gestionnaire d'action MSDTC n'a pas réussi à
extraire la transaction du gestionnaire de transaction source à cause de problèmes de communication.
Causes possibles : un pare-feu est présent et il ne présente pas d'exception pour la procédure MSDTC,
les deux machines ne se trouvent pas avec leur nom NetBIOS ou la prise en charge des transactions de
réseau n'est pas activée pour l'un des gestionnaires de transactions.
```

Cause

Lorsque vous clonez un serveur IaaS sur lequel DTC est déjà installé, le clone contient le même identifiant unique pour DTC que le parent. Échec de la communication entre les deux machines.

Solution

- 1 Sur le clone, ouvrez une invite de commande en tant qu'administrateur.

- 2 Exécutez la commande suivante.

```
msdtc -uninstall
```

- 3 Redémarrez le clone.

- 4 Ouvrez une autre invite de commande et exécutez la commande suivante.

```
msdtc -install manager-service-host-FQDN
```

Le comportement de personnalisation des e-mails a été modifié

Dans vRealize Automation 6.0 ou version ultérieure, seules les notifications générées par le composant IaaS peuvent être personnalisées à l'aide de la fonctionnalité du modèle d'e-mail des versions antérieures.

Solution

Vous pouvez utiliser les modèles XSLT suivants :

- ArchivePeriodExpired
- EpiRegister
- EpiUnregister
- LeaseAboutToExpire
- LeaseExpired
- LeaseExpiredPowerOff
- ManagerLeaseAboutToExpire
- ManagerLeaseExpired
- ManagerReclamationExpiredLeaseModified
- ManagerReclamationForcedLeaseModified
- ReclamationExpiredLeaseModified
- ReclamationForcedLeaseModified
- VdiRegister
- VdiUnregister

Les modèles d'e-mail se trouvent dans le répertoire `\Templates` sous le répertoire d'installation du serveur, généralement `%SystemDrive%\Program Files x86\VMware\vCAC\Server`. Le répertoire `\Templates` contient également des modèles XSLT qui ne sont plus pris en charge et ne peuvent pas être modifiés.

Dépannage des erreurs de connexion

Les rubriques consacrées au dépannage des erreurs de connexion pour vRealize Automation proposent des solutions à des problèmes potentiels liés à l'installation que vous pourriez rencontrer en utilisant vRealize Automation.

Des tentatives de connexion en tant qu'administrateur IaaS avec des informations d'identification au format UPN incorrect échouent sans explication

Vous tentez de vous connecter à vRealize Automation en tant qu'administrateur IaaS et vous êtes redirigé sur la page de connexion sans explication.

Problème

Si vous tentez de vous connecter à vRealize Automation en tant qu'administrateur IaaS avec des informations d'identification UPN qui n'incluent pas la partie *@ votredomaine* du nom d'utilisateur, vous êtes immédiatement déconnecté de SSO et redirigé vers la page de connexion sans explication.

Cause

L'UPN entré doit respecter le format *yourname.admin@yourdomain*, par exemple si vous vous connectez en utilisant *jsmith.admin@sqa.local* comme nom d'utilisateur alors que l'UPN dans Active Directory est défini sur *jsmith.admin*, la connexion échoue.

Solution

Pour corriger le problème, modifiez la valeur `userPrincipalName` pour inclure le contenu *@yourdomain* requis et réessayez. Dans cet exemple, le nom UPN doit être *jsmith.admin@sqa.local*. Cette information est fournie dans le fichier journal du dossier `log/vcac`.

La connexion échoue avec la haute disponibilité

Lorsque vous utilisez plusieurs dispositifs vRealize Automation, ceux-ci doivent pouvoir s'identifier entre eux par un nom d'hôte court. Sinon, vous ne pouvez pas vous connecter.

Pour permettre à un cluster de dispositifs vRealize Automation à haute disponibilité de résoudre des noms d'hôtes courts, adoptez l'une des approches suivantes. Vous devez modifier tous les dispositifs du cluster.

Problème

Vous configurez vRealize Automation pour la haute disponibilité en installant un dispositif vRealize Automation supplémentaire. Lorsque vous tentez de vous connecter à vRealize Automation, un message sur une licence non valide s'affiche. Le message est toutefois incorrect, car vous avez déterminé que votre licence est valide.

Cause

Les nœuds du dispositif vRealize Automation ne forment pas correctement un cluster à haute disponibilité tant qu'ils ne peuvent pas résoudre les noms d'hôtes courts des nœuds du cluster.

Solution

- ◆ Modifiez ou créez une ligne de recherche dans `/etc/resolv.conf`. La ligne doit inclure les domaines qui contiennent les dispositifs vRealize Automation. Quand il y a plusieurs domaines, séparez-les par des espaces. Par exemple :

```
search sales.mycompany.com support.mycompany.com
```

- ◆ Modifiez ou créez des lignes de domaine dans `/etc/resolv.conf`. Chaque ligne doit inclure un domaine qui contient des dispositifs vRealize Automation. Par exemple :

```
domain support.mycompany.com
```

- ◆ Ajoutez des lignes au fichier `/etc/hosts` de telle sorte que chaque nom court de dispositif vRealize Automation soit mappé à son nom de domaine complet. Par exemple :

```
node1    node1.support.mycompany.com
node2    node2.support.mycompany.com
```

Le proxy empêche l'utilisateur de VMware Identity Manager de se connecter

La configuration d'un proxy en vue de son utilisation peut empêcher les utilisateurs de VMware Identity Manager de se connecter.

Conditions préalables

Configurez vRealize Automation pour accéder au réseau via un serveur de proxy. Reportez-vous à [Se connecter au réseau par le biais d'un serveur proxy](#).

Problème

Vous configurez vRealize Automation pour accéder au réseau via un serveur de proxy, et les utilisateurs de VMware Identity Manager voient l'erreur suivante lorsqu'ils tentent de se connecter.

```
Error Unable to get metadata
```

Solution

- 1 Connectez-vous à la console du dispositif vRealize Automation en tant qu'utilisateur racine.
- 2 Ouvrez le fichier suivant dans un éditeur de texte.

```
/etc/sysconfig/proxy
```

- 3 Mettez à jour la ligne NO_PROXY afin d'ignorer le serveur de proxy pour les connexions VMware Identity Manager.

`NO_PROXY=vrealize-automation-hostname`

Par exemple : `NO_PROXY="localhost, 127.0.0.1, automation.mycompany.com"`

- 4 Enregistrez et fermez le proxy.
- 5 Redémarrez le service Horizon Workspace en saisissant la commande suivante.

`service horizon-workspace restart`