

Installation de vRealize Automation

vRealize Automation 7.1

Ce document prend en charge la version de chacun des produits répertoriés, ainsi que toutes les versions publiées par la suite jusqu'au remplacement dudit document par une nouvelle édition. Pour rechercher des éditions plus récentes de ce document, rendez-vous sur :
<http://www.vmware.com/fr/support/pubs>.

FR-002088-04

vmware[®]

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

<http://www.vmware.com/fr/support/>

Le site Web de VMware propose également les dernières mises à jour des produits.

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

docfeedback@vmware.com

Copyright © 2017 VMware, Inc. Tous droits réservés. [Copyright et informations sur les marques.](#)

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

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

Table des matières

Installation de vRealize Automation	7
Informations mises à jour	9
1 Présentation de l'installation de vRealize Automation	11
Choisir votre chemin de déploiement	11
Présentation du déploiement minimal	12
Présentation du déploiement d'entreprise	13
Composants d'installation de vRealize Automation	14
Le dispositif vRealize Automation	15
Agents de gestion	15
Infrastructure vRealize Automation en tant que service	15
2 Préparation à l'installation de vRealize Automation	19
Noms d'hôtes et adresses IP	19
Configuration matérielle et conditions requises de la machine virtuelle	20
Considérations concernant le navigateur	20
Considérations sur les mots de passe	21
Conditions requises pour Windows Server	21
Configuration requise du serveur de la base de données IaaS	21
Exigences relatives au service Web IaaS et au serveur Model Manager	22
IaaS Manager Service	23
Conditions requises pour Distributed Execution Manager	23
Configuration requise du port vRealize Automation	26
Comptes d'utilisateurs et informations d'identification requis pour l'installation	29
Sécurité	30
Certificats	30
Extraction de certificats et de clés privées	31
Phrase secrète de sécurité	31
Logiciels tiers	32
Synchronisation de l'heure	32
3 Installation de vRealize Automation avec l'assistant Installation	33
Déployer le dispositif vRealize Automation	33
Utilisation de l'assistant d'installation pour des déploiements minimaux	35
Exécuter l'assistant d'installation pour un déploiement minimal	35
Installation de l'agent de gestion	36
Synchroniser les heures des serveurs	39
Exécuter l'outil de vérification des conditions préalables	39
Spécifier les paramètres d'un déploiement minimal	40
Créer des snapshots avant de commencer l'installation	40
Scénario : terminer l'installation	40

Échecs de l'installation d'adresse	41
Configurer les informations d'identification pour la configuration de contenu initial	42
Utilisation de l'assistant d'installation pour les déploiements d'entreprise	42
Exécuter l'assistant d'installation pour un déploiement d'entreprise	43
Installation de l'agent de gestion	43
Synchroniser les heures des serveurs	46
Exécuter l'outil de vérification des conditions préalables	46
Spécifier les paramètres d'un déploiement d'entreprise	47
Créer des snapshots avant de commencer l'installation	47
Terminer l'installation	48
Échecs de l'installation d'adresse	48
Configurer les informations d'identification pour la configuration de contenu initial	49
4 Les interfaces d'installation standard de vRealize Automation	51
Utilisation des interfaces standard pour des déploiements minimaux	51
Liste de contrôle pour un déploiement minimal	52
Déployer et configurer le dispositif vRealize Automation	52
Installation des composants IaaS	57
Utilisation des interfaces standard pour les déploiements distribués	63
Liste de contrôle d'un déploiement distribué	63
Composants d'une installation distribuée	64
Désactivation des contrôles de santé de l'équilibrage de charge	65
Exigences d'approbation de certificat dans un déploiement distribué	65
Configurer une approbation de certificat pour des hôtes de composants Web, Manager Service et DEM	66
Feuilles d'activité d'installation	66
Déployer le dispositif vRealize Automation	68
Configuration de votre équilibrage de charge	70
Configuration de dispositifs pour vRealize Automation	70
Installer les composants IaaS dans une configuration distribuée	77
Installation d'agents vRealize Automation	102
Définir la stratégie d'exécution PowerShell sur RemoteSigned	102
Choisir le scénario d'installation de l'agent	103
Emplacement et conditions d'installation de l'agent	103
Installation et configuration de l'agent Proxy pour vSphere	103
Installation de l'agent Proxy pour Hyper-V ou XenServer	109
Installation de l'agent VDI pour XenDesktop	113
Installation de l'agent EPI pour Citrix	116
Installation de l'agent EPI pour les scripts Visual Basic	119
Installation de l'agent WMI pour les demandes WMI à distance	122
5 Tâches post-installation vRealize Automation	125
Remplacement de certificats autosignés par des certificats fournis par une autorité	125
Installation de l'agent vRealize Log Insight sur des serveurs IaaS	125
Configurer l'accès au locataire par défaut	125
6 Dépannage de l'installation de vRealize Automation	127
Emplacement des journaux par défaut	127

Restauration d'une installation qui a échoué	128
Restaurer une installation minimale	129
Restaurer une installation distribuée	129
Création d'un bundle de support vRealize Automation	130
Dépannage de l'installation générale	131
L'installation des mises à niveau échoue avec une erreur de délai d'attente des équilibrages de charge	131
Les heures des serveurs ne sont pas synchronisées	131
Des pages blanches peuvent apparaître lors de l'utilisation d'Internet Explorer 9 ou 10 sur Windows 7	132
Impossible d'établir une relation de confiance pour le canal sécurisé SSL/TLS	132
Se connecter au réseau par le biais d'un serveur proxy	133
Étapes sur la console pour une configuration de contenu initial	133
Dépannage du dispositif vRealize Automation	134
Le téléchargement des programmes d'installation échoue	134
Le fichier Encryption.key comporte des autorisations incorrectes	135
Échec du démarrage d'Identity Manager après le redémarrage de Horizon-Workspace	135
Attributions de rôles de dispositifs incorrectes après basculement	136
Dépannage des composants IaaS	137
Validation des certificats de serveur pour IaaS	137
Erreur d'informations d'identification lors de l'exécution du programme d'installation d'IaaS	138
Un avertissement d'enregistrement des paramètres s'affiche lors de l'installation d'IaaS	138
Échec de l'installation du serveur de site Web et des Distributed Execution Managers	138
L'authentification IaaS échoue lors de l'installation d'IaaS Web et de Model Management	139
L'installation des données Model Manager et des composants Web a échoué	139
Les serveurs Windows IaaS ne prennent pas en charge la norme FIPS	140
L'ajout d'un point de terminaison XaaS génère une erreur interne	141
Échec de la désinstallation de l'agent proxy	141
Les demandes de machine échouent lorsque les transactions à distance sont désactivées	142
Erreur dans la communication de Manager Service	143
Le comportement de personnalisation des e-mails a été modifié	143
Dépannage des erreurs de connexion	144
Des tentatives de connexion en tant qu'administrateur IaaS avec des informations d'identification au format UPN incorrect échouent sans explication	144
La connexion échoue avec la haute disponibilité	144
Le proxy empêche les utilisateurs de VMware Identity Manager de se connecter	145
7 Installation silencieuse de vRealize Automation	147
Effectuer une installation silencieuse de vRealize Automation	147
Effectuer une installation silencieuse de l'agent de gestion de vRealize Automation	148
Fichier de réponses pour installation silencieuse de vRealize Automation	149
La ligne de commande d'installation de vRealize Automation	150
Informations de base sur la ligne de commande d'installation de vRealize Automation	150
Noms des commandes d'installation de vRealize Automation	151
Index	153

Installation de vRealize Automation

vRealize Automation Installation explique comment installer VMware vRealize™ Automation.

REMARQUE 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.

Glossaire VMware Technical Publications

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

Informations mises à jour

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

Révision	Description
FR-002088-04	Autorisation Configurer un cluster de banques de données ajoutée dans « Conditions requises de l'agent vSphere », page 104.
FR-002088-03	<ul style="list-style-type: none">■ Rubrique « Configurer le compte des services Windows pour utiliser l'authentification SQL », page 101 révisée.■ Rubrique « Conditions requises de l'agent vSphere », page 104 révisée.
FR-002088-02	Mises à jour des conditions préalables du serveur Windows IaaS.
FR-002088-01	<ul style="list-style-type: none">■ Ajout de 5480 aux ports IaaS sortants. Reportez-vous à « Configuration requise du port vRealize Automation », page 26.■ Correction de l'emplacement dans lequel créer un bundle de support. Reportez-vous à « Création d'un bundle de support vRealize Automation », page 130.■ Ajout de la configuration requise pour le mode de compatibilité des bases de données SQL Server distinctes. Reportez-vous à « Configuration requise du serveur de la base de données IaaS », page 21.
FR-002088-00	Version de document initiale.

Présentation de l'installation de vRealize Automation

1

Vous pouvez déployer vRealize Automation dans diverses configurations. Pour qu'un déploiement aboutisse, familiarisez-vous avec les options de déploiement et de configuration, ainsi qu'avec la séquence de tâches requise.

Si vous avez installé des versions antérieures de vRealize Automation, notez les modifications suivantes avant de commencer.

- Cette version de vRealize Automation intègre l'assistant d'installation introduit dans vRealize Automation 7.0. Nous recommandons toujours d'utiliser l'assistant pour les installations sans script. L'assistant prend en charge les déploiements minimaux ou distribués.
- Cette version de vRealize Automation introduit une installation avec scripts basée sur console fonctionnant avec un fichier de réponses que vous configurez à l'avance.
- Cette version introduit une interface de ligne de commande pour les tâches d'installation que vous voudrez peut-être effectuer après l'installation initiale, par exemple ajouter un autre vRealize Automation appliance à votre déploiement pour assurer la haute disponibilité.
- Cette version déplace la page de téléchargement du programme d'installation de l'agent logiciel et de l'invité.

<https://vrealize-automation-appliance-FQDN/software/index.html>

Après l'installation, vous commencez à utiliser vRealize Automation en personnalisant l'environnement et en configurant un ou plusieurs locataires, ce qui définit l'accès au provisionnement et à la gestion du cycle de vie des services de cloud en libre-service. Le portail Web sécurisé de vRealize Automation permet aux administrateurs, aux développeurs ou aux utilisateurs d'entreprise de demander des services informatiques et de gérer des ressources de cloud et informatiques spécifiques en fonction de leur rôle et de leurs privilèges. Les utilisateurs demandent une infrastructure, des applications, des postes de travail et des services informatiques grâce à un catalogue de services commun.

Ce chapitre aborde les rubriques suivantes :

- « Choisir votre chemin de déploiement », page 11
- « Composants d'installation de vRealize Automation », page 14

Choisir votre chemin de déploiement

En fonction des conditions requises pour votre déploiement, vous pouvez installer et configurer des composants vRealize Automation en utilisant le scénario d'installation Rainpole, l'assistant d'installation ou la console de gestion.

Choisissez une installation minimale pour déployer une validation technique ou un environnement de développement avec une topologie de base. Choisissez une installation d'entreprise pour déployer un environnement de production ayant la topologie la mieux adaptée aux besoins de votre organisation.

Tableau 1-1. Choisir votre méthode d'installation

Méthode d'installation	Détails
Assistant d'installation	<p>L'assistant d'installation fournit le chemin d'installation le plus rapide pour la plupart des déploiements. Vous pouvez choisir un déploiement minimal ou d'entreprise pour prendre en charge les composants distribués avec ou sans équilibrage de charge. Remplissez et vérifiez toutes les conditions préalables avant de lancer l'assistant.</p> <p>Pour plus d'informations, reportez-vous à Chapitre 2, « Préparation à l'installation de vRealize Automation », page 19.</p>
Installation manuelle	<p>L'installation via la console de gestion est aussi prise en charge pour les installations minimales, distribuées et à haute disponibilité. Remplissez et vérifiez toutes les conditions préalables avant de commencer l'installation.</p> <p>Pour plus d'informations, reportez-vous à Chapitre 2, « Préparation à l'installation de vRealize Automation », page 19.</p> <p>REMARQUE Si vous utilisez la console de gestion pour démarrer ou configurer toute partie de votre installation, vous ne pouvez pas lancer ou continuer à utiliser l'assistant d'installation.</p>
<i>Installation et configuration de vRealize Automation pour le scénario Rainpole</i>	<p>En tant qu'administrateur vSphere, vous voulez installer un déploiement minimal de vRealize Automation dans votre environnement vSphere existant. Vous utilisez l'assistant d'installation pour installer vRealize Automation et créez les éléments de catalogue de contenu initial qui vous aident à configurer rapidement un environnement afin d'utiliser une validation technique.</p> <p>Un déploiement de validation technique ne convient pas à un environnement de production. Lorsque vous effectuez le déploiement de validation technique, vous le configurez comme un environnement de développement dans lequel votre équipe informatique et vous-même créez et testez des Blueprints. Vous pouvez exporter des Blueprints et d'autres éléments conceptuels de votre environnement de développement vers votre environnement de production.</p> <p>Pour commencer ce scénario, consultez <i>Installation et configuration de vRealize Automation pour le scénario Rainpole</i>.</p>

Tableau 1-2. Choisir votre type de déploiement

Objectif du déploiement	Choisir ce type de déploiement
Déployez une validation technique ou un environnement de développement avec une topologie de base.	<p>Installez un déploiement minimal.</p> <p>Vous déployez une instance unique de vRealize Automation appliance et vous installez tous les composants IaaS sur une machine serveur Windows unique. Vous pouvez installer les bases de données sur la même machine Windows ou sur un serveur SQL dédié.</p>
Déployez un environnement de production ayant la topologie la mieux adaptée aux besoins de votre organisation.	<p>Installez un déploiement d'entreprise.</p> <p>Vous répartissez des composants sur plusieurs serveurs. Vous pouvez également déployer des équilibrages de charge pour répartir le travail entre les serveurs et fournir des capacités de basculement et de redondance dans un environnement de haute disponibilité.</p>

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

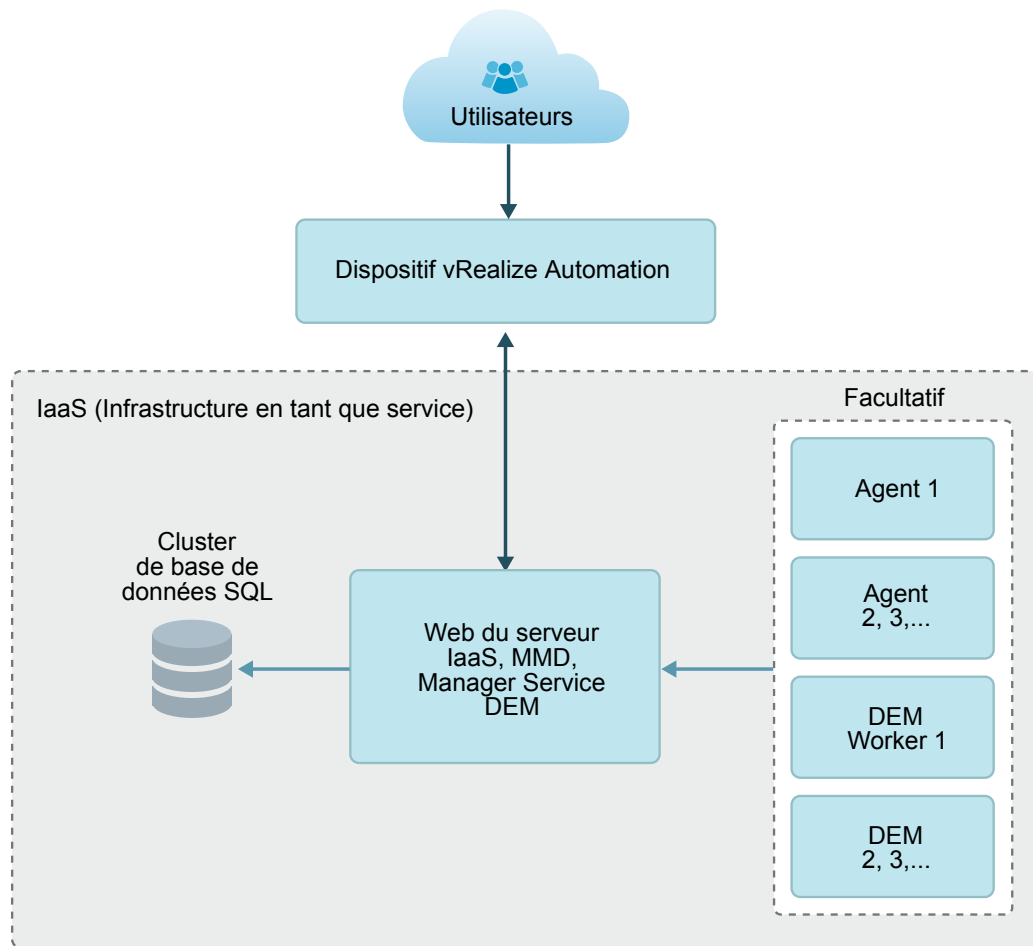
Présentation du déploiement minimal

Pour procéder à un déploiement minimal, un administrateur système doit installer les composants du dispositif vRealize Automation appliance et IaaS (Infrastructure en tant que service).

- Le dispositif vRealize Automation appliance inclut l'interface de la console Web et la prise en charge de capacités de Single Sign-On. Il est installé en tant que dispositif virtuel.
- IaaS (infrastructure en tant que service) est installé sur une machine Windows Server.

- IaaS utilise une base de données SQL pouvant être installée sur la même machine qu'IaaS ou sur son propre serveur.

La figure suivante illustre la relation et l'objectif des composants d'une installation minimale.



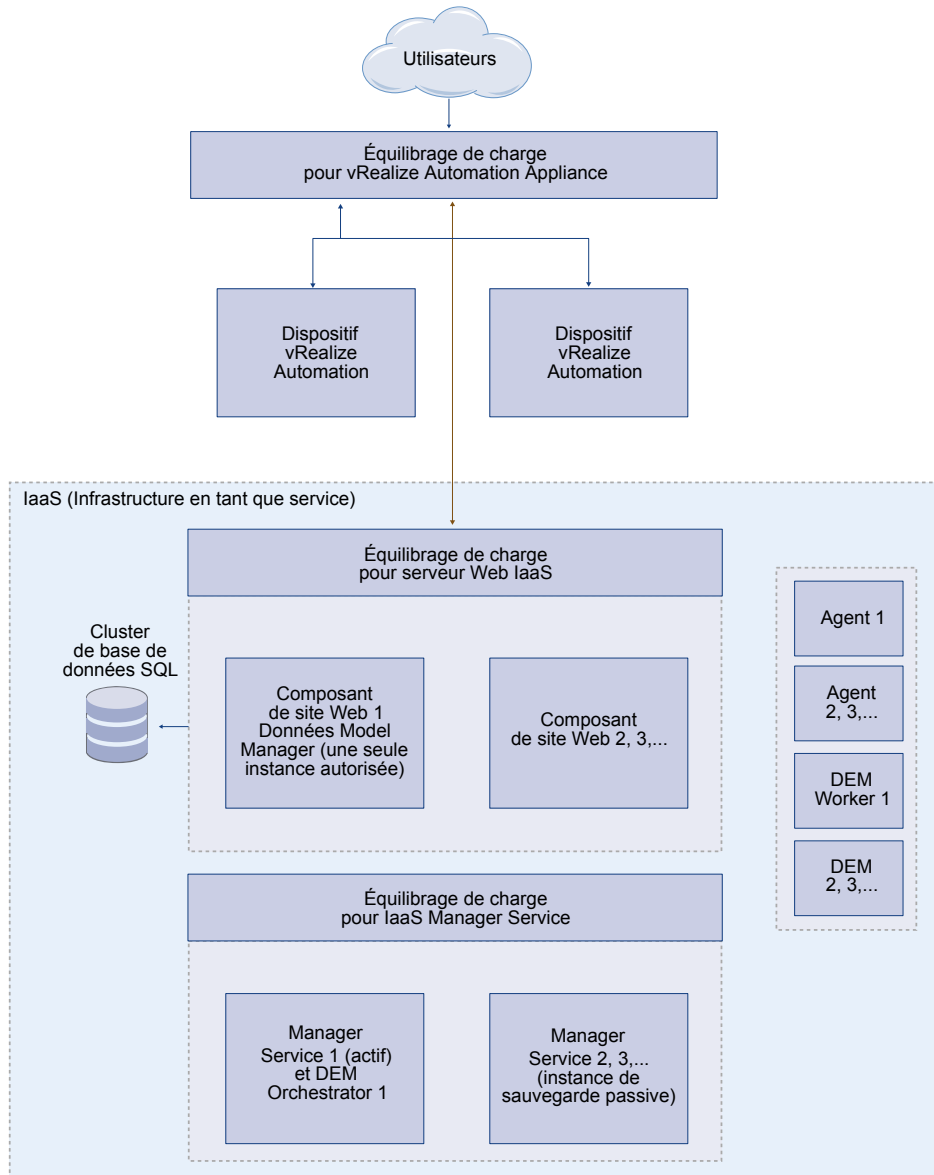
Présentation du déploiement d'entreprise

L'administrateur système peut déployer et installer plusieurs instances du dispositif vRealize Automation appliance et des composants IaaS individuels à des fins de mise à l'échelle, de redondance, de haute disponibilité et de reprise après sinistre.

Dans cette architecture typique, les composants IaaS sont distribués sur plusieurs machines.

Pour les déploiements à haute disponibilité, les équilibres de charge distribuent la charge de travail dans l'environnement informatique. Les administrateurs système configurent les équilibres de charge en dehors de l'infrastructure vRealize Automation.

La figure suivante présente les composants d'un déploiement d'entreprise avec des composants distribués, de la redondance et des équilibres de charge.

Figure 1-1. Configuration du déploiement pour des installations d'entreprise

Composants d'installation de vRealize Automation

Une installation de vRealize Automation inclut l'installation et la configuration des fonctionnalités des composants d'authentification unique (SSO), de portail d'interface et d'infrastructure en tant que service (IaaS).

Une installation est constituée des composants suivants.

- Le dispositif vRealize Automation appliance, qui déploie la console de gestion, gère les capacités Single Sign-On (SSO) pour l'autorisation et l'authentification et comprend une instance de vRealize Orchestrator.
- Les composants d'infrastructure en tant que service (IaaS), qui sont installés sur une machine Windows virtuelle ou physique et qui figurent pour la plupart dans l'onglet **Infrastructure** sur la console.
- Une base de données Microsoft SQL Server, qui est déployée pendant l'installation d'IaaS.

Le dispositif vRealize Automation

Le dispositif vRealize Automation appliance est un dispositif virtuel Linux préconfiguré qui contient le serveur vRealize Automation.

vRealize Automation est fourni sous la forme d'un fichier .ovf ou .ova de virtualisation ouvert. Le dispositif virtuel est déployé sur l'infrastructure virtualisée existante.

Le serveur inclut la console du produit vRealize Automation appliance qui constitue un portail unique pour le provisionnement et une gestion des services de cloud en libre service, la création, l'administration et le contrôle.

Base de données de dispositif

Pendant le déploiement des dispositifs virtuels, une base de données de dispositif PostgreSQL est créée automatiquement sur le premier dispositif vRealize Automation appliance. Une base de données de réplica peut être installée sur un second dispositif vRealize Automation pour permettre la haute disponibilité.

Agents de gestion

Les agents de gestion sont des composants IaaS autonomes qui inscrivent des nœuds IaaS auprès des dispositifs vRealize Automation, automatisent l'installation et la gestion des composants IaaS et collectent des informations de support et de télémétrie.

Un agent de gestion doit être installé sur chaque machine Windows hébergeant des composants IaaS.

Infrastructure vRealize Automation en tant que service

IaaS (Infrastructure en tant que service) vous permet de modéliser et de provisionner rapidement des serveurs et des postes de travail dans des infrastructures privées, publiques ou de cloud hybride.

L'administrateur système installe des composants IaaS sur une machine Windows. Les capacités IaaS sont également disponibles dans l'onglet **Infrastructure** de la console de gestion. IaaS dispose de plusieurs composants que vous pouvez installer dans une configuration personnalisée afin de répondre aux besoins de votre organisation.

Site Web IaaS

Le composant de site Web IaaS fournit les fonctionnalités d'administration d'infrastructure et de création de service à la console vRealize Automation. Le composant de site Web communique avec Manager Service, qui lui fournit des mises à jour du DEM, des agents proxy et de la base de données.

Model Manager

Les modèles vRealize Automation permettent l'intégration à des systèmes et bases de données externes. Ils implémentent une logique métier utilisée par un 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. Il communique avec la base de données, les DEM et le site Web de la console.

Manager Service

Le composant Manager Service 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.

Votre déploiement IaaS nécessite qu'une seule machine Windows exécute de façon active le composant Manager Service. Pour la sauvegarde ou la haute disponibilité, vous devez déployer des machines Windows supplémentaires lorsque vous démarrez manuellement Manager Service si le service actif s'arrête.

IMPORTANT L'exécution simultanée d'un composant Manager Service actif sur plusieurs serveurs Windows IaaS rend vRealize Automation inutilisable.

Le composant Manager Service communique avec le site Web IaaS par le biais de Model Manager et doit s'exécuter sous un compte de domaine avec des privilèges d'administrateur sur toutes les machines IaaS Windows.

Base de données IaaS

Le composant IaaS de vRealize Automation utilise une base de données Microsoft SQL Server pour gérer les informations sur les machines qu'il gère et ses propres éléments et stratégies. Généralement, la base de données est créée pour vous lors de l'installation. Toutefois, un administrateur système peut aussi créer la base de données séparément.

Distributed Execution Manager

Un Distributed Execution Manager (DEM) exécute la logique métier de modèles personnalisés, interagissant avec la base de données et avec des bases de données et des systèmes externes selon les besoins.

Chaque instance DEM s'exécute en tant que travailleur ou en tant qu'instance Orchestrator. Le rôle de l'instance Travailleur est d'exécuter les workflows. Le rôle de l'instance Orchestrator est de surveiller les instances de l'instance DEM Travailleur, de traiter au préalable les workflows à exécuter et de planifier les workflows.

Le DEM Orchestrator effectue ces tâches spécifiques.

- Surveille le statut des instances DEM Travailleur et vérifie que, si une instance Travailleur s'arrête ou perd sa connexion au Model Manager, ses workflows sont remis dans la file d'attente pour qu'une autre instance DEM Travailleur les sélectionne.
- Gère les workflows planifiés en créant de nouvelles instances de workflow au moment planifié.
- Vérifie qu'une seule instance d'un workflow planifié spécifique est exécutée à un moment donné.
- Effectue le traitement préalable des workflows qui sont exécutés, y compris le contrôle des conditions préalables pour les workflows, utilisées dans la mise en œuvre de la fonctionnalité RunOneOnly, et créant l'historique d'exécution des workflows.

Une instance DEM Orchestrator est désignée comme l'instance Orchestrator active qui effectue ces tâches. Étant donné que DEM Orchestrator est essentiel pour exécuter les workflows, installez au moins une instance Orchestrator supplémentaire sur une machine distincte à des fins de redondance. L'instance d'Orchestrator est automatiquement installée sur la machine qui exécute également Manager Service. L'instance DEM Orchestrator supplémentaire surveille le statut de l'instance Orchestrator active afin de la remplacer si celle-ci se déconnecte.

Agents vRealize Automation

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

En général, vous installez l'agent vSphere dans le cadre d'un déploiement. Vous pouvez installer des agents supplémentaires en fonction de la configuration de votre site.

Agents d'intégration

Les agents Virtual desktop integration (VDI) PowerShell permettent à vRealize Automation de s'intégrer à des systèmes externes de bureau virtuel. Pour le moment, les machines virtuelles que vRealize Automation provisionne peuvent être enregistrées avec XenDesktop sur un Desktop Delivery Controller (DDC) Citrix et leurs propriétaires peuvent accéder à l'interface Web XenDesktop depuis vRealize Automation.

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 VDI et EPI requièrent un accès de niveau administrateur aux systèmes externes avec lesquels ils interagissent.

Agents proxy de virtualisation

Les machines virtuelles que vRealize Automation gère sont créées sur des hôtes de virtualisation. vRealize Automation utilise des agents proxy de virtualisation pour envoyer des commandes vers et collecter des données depuis le serveur vSphere ESX, XenServer, ainsi que les hôtes de virtualisation Hyper-V et les machines virtuelles qui y sont provisionnées. Un agent proxy a les caractéristiques suivantes.

- Requiert généralement un accès de niveau administrateur à la plate-forme de virtualisation qu'il gère.
- Communique avec Manager Service.
- Est installé séparément avec son propre fichier de configuration.

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 distants depuis un emplacement central. Il facilite la collecte de données depuis des machines Windows que vRealize Automation gère.

Préparation à l'installation de vRealize Automation

2

Les administrateurs système installent vRealize Automation dans leurs environnements de virtualisation existants. Avant de démarrer l'installation, préparez l'environnement de déploiement pour satisfaire la configuration système requise.

Ce chapitre aborde les rubriques suivantes :

- [« Noms d'hôtes et adresses IP », page 19](#)
- [« Configuration matérielle et conditions requises de la machine virtuelle », page 20](#)
- [« Considérations concernant le navigateur », page 20](#)
- [« Considérations sur les mots de passe », page 21](#)
- [« Conditions requises pour Windows Server », page 21](#)
- [« Configuration requise du port vRealize Automation », page 26](#)
- [« Comptes d'utilisateurs et informations d'identification requis pour l'installation », page 29](#)
- [« Sécurité », page 30](#)
- [« Synchronisation de l'heure », page 32](#)

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.

Lors de l'installation, entrez toujours le nom de domaine complet lors de l'identification ou de la sélection d'une machine. N'entrez pas d'adresses IP.

- 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.

- Pré-planifiez la dénomination des domaines et des machines de façon que les machines vRealize Automation commenceront et se termineront par des lettres (a-z) ou des chiffres (0-9), et contiendront uniquement des lettres, des chiffres ou des traits d'union (-). 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.

- Prévoyez de conserver les noms d'hôtes et les noms de domaine complet que vous avez planifiés pour les systèmes vRealize Automation. La modification d'un nom d'hôte après l'installation rend vRealize Automation inutilisable.
- Il est recommandé de réserver et d'utiliser des adresses IP statiques pour tous les dispositifs vRealize Automation appliance 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 appliance 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.

Configuration matérielle et conditions requises de la machine virtuelle

Votre déploiement doit posséder les ressources système minimales pour installer des dispositifs virtuels et la configuration matérielle minimale pour installer des composants IaaS sur le serveur Windows.

Pour connaître les conditions préalables en matière de système d'exploitation et d'environnement de niveau élevé, et pour obtenir des informations sur les navigateurs et systèmes d'exploitation pris en charge, reportez-vous à *Matrice de prise en charge de vRealize Automation*.

Le tableau de configuration matérielle minimale affiche les conditions requises minimales pour le déploiement de dispositifs virtuels et l'installation de composants IaaS. Les dispositifs sont des machines virtuelles préconfigurées que vous ajoutez à votre inventaire vCenter Server ou ESXi. Les composants IaaS sont installés sur des serveurs Windows 2008 R2 SP1 ou Windows 2012 R2 physiques ou virtuels.

Un annuaire Active Directory est considéré comme petit quand l'UO contient près de 25 000 utilisateurs à synchroniser dans la configuration du magasin d'ID. Un annuaire Active Directory est considéré comme large quand l'unité d'organisation contient plus de 25 000 utilisateurs.

Tableau 2-1. Configuration matérielle requise

vRealize Automation appliance pour les petits annuaires Active Directory	vRealize Automation appliance pour les grands annuaires Active Directory	Composants IaaS (serveur Windows).
<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 	<ul style="list-style-type: none"> ■ 2 CPU ■ 8 Go de mémoire ■ 30 Go de stockage sur disque <p>Des ressources supplémentaires sont requises lorsque vous incluez un serveur SQL dans un hôte Windows.</p>

Considérations concernant le navigateur

L'utilisation du navigateur avec vRealize Automation est soumise à certaines restrictions.

- 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 en charge un sous-ensemble de navigateurs vRealize Automation pris en charge.

Pour connaître les conditions préalables en matière de système d'exploitation et d'environnement de niveau élevé, et pour obtenir des informations sur les navigateurs et systèmes d'exploitation pris en charge, reportez-vous à *Matrice de prise en charge de vRealize Automation*.

Considérations sur les mots de passe

Des limitations de caractères s'appliquent à certains mots de passe.

Le mot de passe de l'administrateur VMware vRealize™ Automation ne peut pas contenir de caractère « = » de fin. Ces mots de passe sont acceptés lorsque vous les attribuez, mais ils entraînent des erreurs quand vous effectuez des opérations comme l'enregistrement de points de terminaison.

Conditions requises pour Windows Server

La machine Windows virtuelle ou physique qui héberge les composants IaaS doit respecter la configuration requise de la base de données IaaS, des composants du serveur IaaS, de Manager ServiceIaaS et des Distributed Execution Managers.

L'assistant d'installation exécute l'outil de vérification des conditions préalables devRealize Automation sur tous les serveurs Windows IaaS pour veiller à ce qu'ils respectent la configuration nécessaire à l'installation. Outre l'outil de vérification des conditions préalables, traitez les conditions préalables suivantes de façon séparée.

- Nous recommandons de placer tous les serveurs Windows IaaS dans le même domaine.
- Créez ou identifiez un compte de domaine à utiliser pour l'installation, ce domaine devant avoir des privilèges d'administrateur sur tous les serveurs WindowsIaaS.

Configuration requise du serveur de la base de données IaaS

Le serveur Windows qui héberge la base de données IaaS SQL Server de vRealize Automation doit respecter certaines conditions préalables.

La configuration requise s'applique si vous exécutez l'assistant d'installation ou le programme d'installation `setup_vrealize-automation-appliance-URL.exe` hérité et que vous sélectionnez le rôle de la base de données pour l'installation. Les conditions préalables s'appliquent également si vous créez séparément une base de données SQL Server vide à utiliser avec IaaS.

- Utilisez une version de SQL Server prise en charge du *Matrice de prise en charge de vRealize Automation*.
- Activez le protocole TCP/IP pour SQL Server.
- Activez le service DTC (Distributed Transaction Coordinator) sur tous les serveurs Windows IaaS et la machine hébergeant SQL Server. IaaS utilise DTC pour les transactions de base de données et les actions telles que la création de workflows.

REMARQUE 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](#) », page 143.

Pour plus d'informations sur l'activation de DTC, reportez-vous à l'[article 2038943 de la base de connaissances VMware](#).

- Ouvrez les ports compris entre tous les serveurs Windows IaaS et la machine hébergeant SQL Server. Reportez-vous à « [Configuration requise du port vRealize Automation](#) », page 26.

Sinon, si les stratégies du site le permettent, vous pouvez désactiver les pare-feu situés entre les serveurs Windows IaaS et SQL Server.

- Cette édition de vRealize Automation ne prend pas en charge le mode de compatibilité 130 de SQL Server 2016. 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 d'un programme d'installation vRealize Automation, la compatibilité est déjà configurée.

- La fonctionnalité Groupes de disponibilité AlwaysOn (AAG) est prise en charge avec SQL Server 2016 uniquement.

Exigences relatives au service Web IaaS et au serveur Model Manager

Votre environnement doit répondre aux conditions requises pour les logiciels et la configuration qui prennent en charge l'installation des composants de serveur IaaS.

Exigences relatives à l'environnement et à la base de données pour IaaS

La configuration de votre hôte et votre base de données MS SQL doivent respecter les exigences suivantes.

Tableau 2-2. Conditions requises pour IaaS

Zone	Configuration requise
Configuration d'hôte	<p>Les composants suivants doivent être installés sur l'hôte avant d'installer IaaS :</p> <ul style="list-style-type: none"> ■ Microsoft .NET Framework 4.5.2 ou version ultérieure. ■ Microsoft PowerShell 2.0 (inclus avec Windows Server 2008 R2 SP1 et version ultérieure) ou Microsoft PowerShell 3.0 sur Windows Server 2012 R2. ■ Microsoft Internet Information Services 7.5. ■ Java doit être installé sur la machine exécutant le composant Web principal pour prendre en charge le déploiement de la base de données MS SQL pendant l'installation.
Conditions requises pour la base de données Microsoft SQL	<p>La base de données SQL peut résider sur l'un de vos serveurs IaaS Windows ou sur un hôte distinct.</p> <p>Si la base de données SQL est l'un de vos serveurs IaaS Windows, procédez à la configuration suivante pour satisfaire les conditions requises Java.</p> <ul style="list-style-type: none"> ■ Installez Java 64 bits 1.8 ou version ultérieure. N'utilisez pas la version 32 bits. ■ 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.

Exigences relatives à Microsoft Internet Information Services

Configurez Internet Information Services (IIS) conformément aux exigences suivantes.

Outre les paramètres de configuration, évitez d'héberger des sites Web supplémentaires dans IIS sur l'hôte du serveur Web IaaS. 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 2-3. Configuration requise pour Microsoft Internet Information Services

Composant IIS	Configuration
Modules Internet Information Services (IIS) installés	<ul style="list-style-type: none"> ■ WindowsAuthentication ■ StaticContent ■ DefaultDocument ■ ASPNET 4.5 ■ ISAPIExtensions ■ ISAPIFilter
Paramètres d'authentification IIS	<ul style="list-style-type: none"> ■ Authentification Windows activée ■ Authentification anonyme désactivée ■ 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 serveurs Windows 2012 ou Windows 2012 R2
Service d'activation des processus IIS Windows	<ul style="list-style-type: none"> ■ ConfigurationApi ■ NetEnvironment ■ ProcessModel ■ WcfActivation (Windows 2008 uniquement) ■ HttpActivation ■ NonHttpActivation

IaaS Manager Service

Votre environnement doit répondre à des conditions requises générales qui prennent en charge l'installation de IaaS Manager Service.

- Microsoft .NET Framework 4.5.2 est installé.
- Microsoft PowerShell 2.0, 3.0 ou 4.0. 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.
- Le service Secondary Logon est en cours d'exécution.
- Il ne peut pas y avoir de pare-feu entre l'hôte DEM et le serveur Windows. Pour plus d'informations, reportez-vous à la section « [Configuration requise du port vRealize Automation](#) », page 26.
- IIS est installé et configuré.

Conditions requises pour Distributed Execution Manager

Votre environnement doit respecter certaines spécifications générales qui prennent en charge l'installation des instances Distributed Execution Manager (DEM).

- Microsoft .NET Framework 4.5.2 est installé.
- Microsoft PowerShell 2.0, 3.0 ou 4.0. 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.
- Le service Secondary Logon est en cours d'exécution.

- Aucun pare-feu entre l'hôte DEM et le serveur Windows, ou ports ouverts comme il est décrit dans « [Configuration requise du port vRealize Automation](#) », page 26.

Les serveurs hébergeant les instances DEM Worker peuvent avoir des conditions requises supplémentaires, selon les ressources de provisionnement avec lesquelles elles interagissent.

Configuration requise pour Amazon Web Services EC2

Le serveur vRealize Automation IaaS Windows communique avec un compte Amazon EC2 et collecte des données sur ce compte.

Lorsque vous utilisez les services Web Amazon pour le provisionnement, les serveurs qui hébergent les serveurs IaaS Windows doivent disposer de la configuration requise suivante.

- Les hôtes DEM Worker doivent disposer d'un accès Internet.
- Si les hôtes DEM Worker se trouvent 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 les hôtes DEM Worker ont accès à Internet par le biais d'un serveur proxy, le service DEM doit s'exécuter sous des informations d'identification pouvant être authentifiées sur le serveur proxy.

Configuration requise pour Openstack et PowerVC

Les machines sur lesquelles vous installez vos DEM doivent répondre à certaines spécifications pour communiquer avec votre instance d'Openstack ou de PowerVC et collecter des données depuis celle-ci.

Tableau 2-4. configuration requise pour un hôte DEM

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> <p>[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319] "SchUseStrongCrypto"=dword:00000001</p>
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> <p>[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server] "DisabledByDefault"=dword:00000000 "Enabled"=dword:00000001</p>
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>

Configuration requise de Red Hat Enterprise Virtualization KVM (RHEV)

Quand vous utilisez Red Hat Enterprise Virtualization pour le provisionnement, le serveur IaaS Windows communique avec ce compte et en collecte des données.

Votre environnement doit répondre aux exigences suivantes de Red Hat Enterprise.

- Chaque environnement KVM (RHEV) doit être associé au domaine contenant le serveur IaaS.
- Les informations d'identification utilisées pour gérer le point de terminaison représentant un environnement KVM (RHEV) doivent disposer des privilèges d'administrateur dans l'environnement RHEV. Ces informations d'identification doivent également disposer de suffisamment de privilèges pour créer des objets sur les hôtes dans l'environnement.

Conditions requises de SCVMM

Tous les DEM Workers utilisés pour gérer des machines virtuelles avec SCVMM doivent être installés sur un hôte sur lequel la console SCVMM est déjà installée.

De plus, les conditions requises suivantes doivent être respectées :

- Le DEM doit avoir accès au module SCVMM PowerShell installé avec la console.

- La stratégie d'exécution de MS PowerShell doit être définie sur RemoteSigned ou Unrestricted.

Pour plus d'informations sur la stratégie d'exécution de PowerShell, exécutez l'une des commandes suivantes à l'invite de commande PowerShell :

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

- Si tous les DEM Workers de l'instance ne se trouvent pas sur des ressources de calcul respectant ces conditions requises, des compétences doivent être utilisées pour diriger tous les workflows liés à SCVMM vers celles qui s'y trouvent.

Les conditions requises supplémentaires suivantes s'appliquent à SCVMM.

- Vous devez installer la console SCVMM avant d'installer des DEM Workers qui consomment des éléments de travail SCVMM.

Si vous installez DEM Worker avant la console SCVMM, des journaux d'erreurs similaires à ce qui suit 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. Ces informations d'identification doivent également donner droit aux privilèges d'administrateur sur les serveurs Hyper-V au sein de l'instance.
- 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 des machines sur une ressource de calcul SCVMM, un utilisateur doit être ajouté à au moins un rôle de sécurité dans l'instance de SCVMM.

Configuration requise du port vRealize Automation

vRealize Automation utilise des ports dédiés à la communication et l'accès aux données.

Bien que vRealize Automation utilise uniquement le port 443 pour la communication, d'autres ports peuvent être ouverts sur le système. Étant donné que les ports ouverts non sécurisés peuvent présenter des vulnérabilités au niveau de la sécurité, assurez-vous que seuls les ports nécessaires aux applications de votre entreprise sont ouverts.

Dispositif vRealize Automation

Les ports suivants sont utilisés par le dispositif vRealize Automation appliance.

Tableau 2-5. Ports entrants du dispositif vRealize Automation appliance

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

Tableau 2-5. Ports entrants du dispositif vRealize Automation appliance (suite)

Port	Protocole	Commentaires
111	TCP, UDP	RPC.
443	TCP	Accès à la console vRealize Automation et aux appels d'API.
443	TCP	Accès permettant aux machines de télécharger l'agent invité et l'agent de démarrage logiciel.
5480	TCP	Accès à l'interface de gestion Web du dispositif virtuel.
5480	TCP	Utilisé par l'agent de gestion.
5488, 5489	TCP	Utilisé en interne par le dispositif vRealize Automation appliance pour les mises à jour.
4369, 25672, 5671, 5672	TCP	Messagerie RabbitMQ.
8230, 8280, 8281	TCP	Instance de vRealize Orchestrator interne.
8444	TCP	Communication du proxy de console pour les connexions de VMware Remote Console pour vSphere.

Tableau 2-6. Ports sortants du dispositif vRealize Automation

Port	Protocole	Commentaires
25, 587	TCP, UDP	SMTP pour l'envoi d'e-mails de notification sortants.
53	TCP, UDP	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.
110, 995	TCP, UDP	POP pour recevoir des e-mails de notification entrants.
143, 993	TCP, UDP	IMAP pour recevoir des e-mails de notification entrants.
123	TCP, UDP	Facultatif. Pour la connexion directe au NTP au lieu d'utiliser l'heure de l'hôte.
443	TCP	Communication avec IaaS Manager Service et les hôtes des points de terminaison de l'infrastructure sur HTTPS.
443	TCP	Communication avec l'agent de démarrage logiciel sur HTTPS.
902	TCP	Opérations de copie de fichiers réseau ESXi et connexions de VMware Remote Console.
5050	TCP	Facultatif. Pour communiquer avec vRealize Business.
5432	TCP, UDP	Facultatif. Pour les communications avec Appliance Database.
8281	TCP	Facultatif. Pour communiquer avec une instance de vRealize Orchestrator externe.

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.

IaaS (Infrastructure en tant que service)

Les ports situés dans les tableaux Ports entrants des composants IaaS et Ports sortants de l'infrastructure en tant que service doivent être disponibles pour être utilisés par le serveur Windows Server IaaS.

Tableau 2-7. Ports entrants pour les composants IaaS

Composant	Port	Protocole	Commentaires
Manager Service	443	TCP	Communication avec les composants IaaS et le dispositif vRealize Automation appliance sur HTTPS.
vRealize Automation appliance	443	TCP	Communication avec les composants IaaS et le dispositif vRealize Automation appliance sur HTTPS.
Hôtes des points de terminaison de l'infrastructure	443	TCP	Communication avec les composants IaaS et le dispositif vRealize Automation appliance 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.
Instance du serveur SQL Server	1433	TCP	MSSQL.

Tableau 2-8. Ports sortants pour les composants IaaS

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

Service de coordinateur de transaction distribué Microsoft

En plus de vérifier que les ports répertoriés dans les tableaux précédents sont disponibles, vous devez activer la communication du Service de coordinateur de transaction distribué Microsoft (MS DTC) entre tous les serveurs du déploiement. MS DTC nécessite l'utilisation du port 135 sur TCP et un port aléatoire entre 1024 et 65535.

L'outil de vérification des conditions préalables valide si MS DTC s'exécute et si les ports requis sont ouverts.

Comptes d'utilisateurs et informations d'identification requis pour l'installation

Vous devez vérifier que vous disposez des rôles et informations d'identification vous permettant d'installer des composants vRealize Automation.

Compte de service vCenter

Si vous prévoyez d'utiliser un point de terminaison vSphere, vous avez besoin d'un compte de domaine ou local ayant le niveau d'accès approprié configuré dans vCenter.

Installation de dispositif virtuel

Pour déployer le dispositif vRealize Automation appliance, vous devez disposer de privilèges appropriés sur la plate-forme de déploiement (par exemple, informations d'identification vSphere).

Pendant le processus de déploiement, vous spécifiez le mot de passe du compte d'administrateur du dispositif virtuel. Ce compte offre l'accès à la console de gestion des dispositifs vRealize Automation appliance depuis lesquelles vous configurez et gérez les dispositifs virtuels.

Installation d'IaaS

Avant d'installer des composants IaaS, ajoutez l'utilisateur avec lequel vous prévoyez d'exécuter les programmes d'installation d'IaaS sur le groupe Administrateur de l'hôte d'installation.

Informations d'identification de la base de données IaaS

Vous pouvez créer la base de données pendant l'installation du produit ou manuellement dans le serveur SQL.

Lorsque vous créez ou que vous renseignez une base de données MS SQL via vRealize Automation, que ce soit à l'aide de l'assistant d'installation ou de la console de gestion, les conditions suivantes s'appliquent :

- Si vous utilisez l'option **Utiliser l'authentification Windows**, le rôle **sysadmin** du serveur SQL doit être attribué à l'utilisateur exécutant l'agent de gestion sur le serveur Web IaaS principal afin de créer et de modifier la taille de la base de données.
- Si vous n'utilisez pas l'option **Utiliser l'authentification Windows**, le rôle **sysadmin** du serveur SQL doit également être attribué à l'utilisateur exécutant l'agent de gestion sur le serveur Web IaaS principal. Les informations d'identification sont utilisées lors de l'exécution.
- Si vous renseignez une base de données créée préalablement via vRealize Automation, les informations d'identification d'utilisateur que vous fournissez (l'utilisateur Windows actuel ou l'utilisateur SQL spécifié) nécessitent uniquement les privilèges **dbo** pour base de données IaaS.

REMARQUE Les utilisateurs de vRealize Automation nécessitent également le niveau adéquat d'accès à l'authentification Windows pour se connecter et utiliser vRealize Automation.

Informations d'identification d'utilisateur du service IaaS

IaaS installe plusieurs services Windows qui partagent un seul utilisateur de service.

Les conditions requises suivantes s'appliquent à l'utilisateur des services IaaS :

- L'utilisateur doit être un utilisateur de domaine.

- L'utilisateur doit disposer de privilèges d'administrateur local sur tous les hôtes sur lesquels le composant Manager Service ou de site Web est installé. N'effectuez pas d'installation de groupe de travail.
- L'utilisateur est configuré avec des privilèges **Ouvrir une session en tant que service**. Ce privilège garantit que Manager Service démarre et génère des fichiers journaux.
- L'utilisateur doit disposer de privilèges **dbo** pour la base de données IaaS. Si vous utilisez le programme d'installation pour créer la base de données, vérifiez que l'identifiant de l'utilisateur du service est ajouté au serveur SQL avant d'exécuter le programme d'installation. Le programme d'installation accorde à l'utilisateur du service des privilèges **dbo** après la création de la base de données.
- Le programme d'installation est exécuté sous le compte opérant l'agent de gestion sur le serveur Web principal. Si vous souhaitez utiliser le programme d'installation pour créer une base de données MS SQL lors de l'installation, le rôle **sysadmin** doit être activé dans MS SQL. Cela n'est pas une exigence si vous choisissez d'utiliser une base de données de données vide pré-crée.
- Le compte d'utilisateur de domaine que vous prévoyez d'utiliser comme identité du pool d'applications IIS pour le service Web Model Manager est configuré avec les privilèges **Ouvrir une session en tant que traitement par lots**.

Spécifications du serveur Model Manager

Spécifiez le nom du serveur Model Manager avec un nom de domaine complet. N'utiliser pas d'adresse IP pour spécifier le serveur.

Sécurité

vRealize Automation utilise le protocole SSL pour sécuriser la communication entre les composants. Des phrases secrètes sont utilisées pour le stockage sécurisé des bases de données.

Pour plus d'informations, reportez-vous à « [Exigences d'approbation de certificat dans un déploiement distribué](#) », page 65.

Certificats

vRealize Automation utilise des certificats SSL pour la communication sécurisée entre les composants IaaS et les instances de vRealize Automation appliance. 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 des informations importantes sur la résolution des problèmes, la prise en charge et les conditions d'approbation des certificats, reportez-vous à [l'article 2106583 de la base de connaissances VMware](#).

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 2-9. 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.
Composants 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.

Extraction de certificats et de clés privées

Les certificats que vous utilisez avec les dispositifs virtuels doivent être dans le format de fichier PEM.

Les exemples dans le tableau suivant utilisent les commandes GNU `openssl` pour extraire les informations des certificats que vous devez configurer sur les dispositifs virtuels.

Tableau 2-10. Modèle de valeurs de certificat et de commandes (openssl)

L'autorité de certification fournit	Commande	Entrées de dispositif virtuel
Clé privée RSA	<code>openssl pkcs12 -in path_to_pfx_certificate_file -nocerts -out key.pem</code>	Clé privée RSA
Fichier PEM	<code>openssl pkcs12 -in path_to_pfx_certificate_file -clcerts -nokeys -out cert.pem</code>	Chaîne de certificat
(Facultatif) Phrase secrète	s/o	Phrase secrète

Phrase secrète de sécurité

vRealize Automation utilise des phrases secrètes de sécurité pour sécuriser la base de données. Une phrase secrète est une série de mots utilisés pour créer une phrase qui génère la clé de chiffrement qui protège les données stockées dans la base de données.

Lorsque vous créez une phrase secrète de sécurité pour la première fois, suivez les instructions suivantes.

- Utilisez la même phrase secrète dans l'ensemble de l'installation pour vous assurer que chaque composant dispose de la même clé de chiffrement.
- Utilisez une phrase dont la longueur est supérieure à huit caractères.
- Incluez des majuscules, des minuscules et des chiffres, ainsi que des symboles.

- Mémorisez la phrase secrète ou conservez-la en lieu sûr. La phrase secrète est nécessaire pour restaurer les informations de la base de données en cas de défaillance du système ou pour ajouter des composants suite à l'installation initiale. Sans cette phrase secrète, vous ne pouvez pas effectuer de restauration.

Logiciels tiers

Certains composants de vRealize Automation dépendent de logiciels tiers, notamment Microsoft Windows et SQL Server. Pour vous protéger des failles de sécurité des produits tiers, vérifiez que votre logiciel est à jour avec les derniers correctifs du fournisseur.

Synchronisation de l'heure

Un administrateur système doit configurer un chronométrage précis dans le cadre de l'installation de vRealize Automation.

L'installation échoue si la synchronisation de l'heure n'est pas configurée correctement.

Le chronométrage doit être cohérent et synchronisé entre le dispositif vRealize Automation appliance et les serveurs Windows. Vous pouvez vous assurer de cette cohérence en utilisant la même méthode chronométrage pour chaque composant.

Pour les machines virtuelles, vous pouvez utiliser les méthodes suivantes :

- Configuration à l'aide du Protocole NTP (directement).
- Configuration à l'aide du Protocole NTP via ESXi avec VMware Tools. Vous devez disposer de la configuration du protocole NTP sur ESXi.

Pour les serveurs Windows, reportez-vous à l'article [Timekeeping best practices for Windows, including NTP](#) dans la base de connaissances VMware.

Installation de vRealize Automation avec l'assistant Installation

3

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 vRealize Automation appliance et configurer les serveurs Windows IaaS conformément aux conditions préalables. L'assistant d'installation s'affiche lors de votre première connexion au vRealize Automation appliance 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 4, « Les interfaces d'installation standard de vRealize Automation »](#), page 51.

Ce chapitre aborde les rubriques suivantes :

- [« Déployer le dispositif vRealize Automation »](#), page 33
- [« Utilisation de l'assistant d'installation pour des déploiements minimaux »](#), page 35
- [« Utilisation de l'assistant d'installation pour les déploiements d'entreprise »](#), page 42

Déployer le dispositif vRealize Automation

Pour déployer le dispositif vRealize Automation appliance, un administrateur système doit se connecter au client vSphere et sélectionner les paramètres de déploiement.

Certaines restrictions s'appliquent au mot de passe racine que vous avez créé pour l'administrateur de vRealize Automation.

Prérequis

- Téléchargez le dispositif vRealize Automation appliance sur le site Web VMware.
- Connectez-vous au client vSphere en tant qu'utilisateur disposant des privilèges d'administrateur système.

Procédure

- 1 Sélectionnez **Fichier > Déployer un modèle OVF** depuis le client vSphere.
- 2 Accédez au fichier vRealize Automation appliance que vous avez téléchargé et cliquez sur **Ouvrir**.
- 3 Cliquez sur **Suivant**.

- 4 Sur la page des détails du modèle OVF, cliquez sur **Suivant**.
- 5 Acceptez le contrat de licence, puis cliquez sur **Suivant**.
- 6 Entrez un nom de dispositif virtuel unique conformément à la convention d'affectation de noms de votre organisation dans la zone de texte **Nom**, sélectionnez le centre de données et l'emplacement dans lequel vous souhaitez déployer le dispositif virtuel et cliquez sur **Suivant**.
- 7 Suivez les invites jusqu'à ce que la page Format de disque apparaisse.
- 8 Sur la page Format de disque, vérifiez que l'espace est suffisant pour déployer le dispositif virtuel et cliquez sur **Suivant**.
- 9 Suivez les invites jusqu'à la page Propriétés.

Les options qui apparaissent dépendent de votre configuration vSphere.

- 10 Configurez les valeurs sur la page Propriétés.
 - a Entrez le mot de passe racine qui doit être utilisé pour se connecter à la console du dispositif virtuel dans les zones de texte **Entrer le mot de passe** et **Confirmer le mot de passe**.
 - b Cochez ou décochez la case **Service SSH** pour choisir si le service SSH est activé ou non pour le dispositif.

 Cette valeur permet de définir le statut initial du service SSH dans le dispositif. Si vous installez l'assistant d'installation, activez cette option avant de l'exécuter. Vous pouvez modifier ce paramètre depuis la console de gestion du dispositif après l'installation.
 - c Entrez le nom de domaine complet de la machine virtuelle dans la zone de texte **Nom d'hôte**.
 - d Configurez les propriétés du réseau.
- 11 Cliquez sur **Suivant**.
- 12 Selon votre déploiement, vCenter, et la configuration de DNS, sélectionnez l'une des manières suivantes de terminer le déploiement OVA et la mise sous tension de vRealize Automation appliance.
 - 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 le déploiement des fichiers effectué dans vCenter, cliquez sur **Fermé**.
 - c Attendez le démarrage de la machine, qui peut durer 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 le déploiement des fichiers effectué dans vCenter, cliquez sur **Fermé**.
 - b Mettez sous-tension le dispositif vRealize Automation appliance.
 - c Attendez le démarrage de la machine, qui peut durer jusqu'à 5 minutes.
 - d Vérifiez que vous pouvez effectuer un test ping sur le serveur DNS du dispositif vRealize Automation appliance. Dans le cas contraire, redémarrez la machine virtuelle.
 - e Attendez le démarrage de la machine, qui peut durer jusqu'à 5 minutes.
 - Si vous avez déployé le dispositif vRealize Automation appliance 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 appliance.
 - b Cliquez avec le bouton droit sur le dispositif vRealize Automation appliance, 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 appliance.
 - f Attendez le démarrage de la machine, qui peut durer jusqu'à 5 minutes.
- 13 Ouvrez une invite de commande et effectuez un test ping sur le nom de domaine complet pour vérifier que celui-ci peut être résolu sur l'adresse IP de vRealize Automation appliance.

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

Exécuter l'assistant d'installation pour un déploiement minimal

Installez un déploiement minimal pour le travail de validation technique. Dans le cas d'une installation minimale, l'assistant considère que vous installez tous les composants IaaS sur une seule machine Windows.

Les déploiements minimaux prennent généralement en charge une seule instance de vRealize Automation appliance et un serveur IaaS, et ils utilisent un agent vSphere pour prendre en charge les points de terminaison.

Prérequis

- Vérifiez que toutes les conditions préalables décrites dans [Chapitre 2, « Préparation à l'installation de vRealize Automation »](#), page 19 sont satisfaites.
- [« Déployer le dispositif vRealize Automation »](#), page 68

Procédure

- 1 Ouvrez un navigateur Web.
- 2 Accédez à la console de gestion de vRealize Automation appliance en utilisant son nom de domaine complet (<https://vra-va-hostname.domain.name:5480/>).
- 3 Connectez-vous à l'aide du nom d'utilisateur **racine** et du mot de passe que vous avez spécifiés lorsque le dispositif a été déployé.
- 4 Lorsque l'assistant d'installation s'affiche, cliquez sur **Suivant**.
- 5 Acceptez le contrat de licence d'utilisateur final, puis cliquez sur **Suivant**.
- 6 Sélectionnez **Déploiement minimal** et **Installer les infrastructures en tant que service** sur l'écran Type de déploiement, puis cliquez sur **Suivant**.
- 7 Vérifiez que les conditions préalables mentionnées sur la page Conditions préalables d'installation sont satisfaites et que les serveurs Windows sur lesquels vous installez l'agent de gestion sont indiqués.
- 8 Si besoin, vous pouvez modifier la méthode de chronométrage pour votre dispositif vRealize Automation. Cliquez sur **Modifier les paramètres d'heure** si vous réalisez des modifications.
- 9 Cliquez sur **Suivant**.

- 10 Cliquez sur **Exécuter** dans l'écran Exécuter l'outil de vérification des conditions préalables pour vérifier que le serveur Windows de votre déploiement minimal est correctement configuré pour l'utilisation avec vRealize Automation.

Puisque cette étape s'exécute à distance, plusieurs minutes peuvent être nécessaires à son exécution.

- a Si un état indiquant un échec est envoyé pour une machine, cliquez sur **Corriger** démarrer la réparation automatique ou sur **Afficher les détails** et suivez les instructions.

L'option **Corriger** applique des corrections et redémarre le serveur Windows IaaS.

- b Cliquez sur **Exécuter** pour exécuter une nouvelle fois le contrôleur.
 - c Quand aucun échec n'est indiqué, cliquez sur **Suivant**.
- 11 Passez aux écrans suivants, en fournissant les informations requises pour configurer vos composants de déploiement, y compris le serveur Web, Manager Service, Distributed Execution Manager, l'agent de proxy vSphere et les informations de certificat.

Des informations supplémentaires sont disponibles depuis les bouton de l'Aide.

Suivant

[« Créer des snapshots avant de commencer l'installation », page 40](#)

Installation de l'agent de gestion

Vous devez installer un agent de gestion sur chaque machine Windows hébergeant des composants IaaS.

Pour les installations d'entreprise, aucun agent de gestion n'est requis pour l'hôte MS SQL.

Si votre dispositif vRealize Automation principal échoue, vous devez réinstaller des agents de gestion.

Les agents de gestion ne sont pas automatiquement supprimés lorsque vous désinstallez un composant IaaS. Désinstallez l'agent de gestion de la même manière que vous désinstalleriez un programme Windows au moyen de l'outil Ajouter ou supprimer des programmes.

Procédure

- 1 [Trouver l'empreinte digitale de certificat SSL pour le service du site de gestion.](#) page 36
Lorsque vous installez un agent de gestion, vous devez valider l'empreinte digitale du certificat SSL pour le service du site de gestion.
- 2 [Télécharger et installer un agent de gestion](#) page 37
Un administrateur télécharge et installe l'agent de gestion sur la machine IaaS de votre déploiement. L'agent de gestion doit être installé sur le serveur IaaS mais ne doit pas nécessairement être installé sur le serveur de la base de données SQL s'il est séparé.

Trouver l'empreinte digitale de certificat SSL pour le service du site de gestion.

Lorsque vous installez un agent de gestion, vous devez valider l'empreinte digitale du certificat SSL pour le service du site de gestion.

Vous pouvez obtenir l'empreinte digitale à l'invite de commandes sur vRealize Automation appliance.

Procédure

- 1 Connectez-vous à la console vRealize Automation appliance en tant que racine.

- 2 Entrez la commande suivante :

```
openssl x509 -in /opt/vmware/etc/lighttpd/server.pem -fingerprint -noout -sha1
```

L'empreinte digitale SHA1 s'affiche. Par exemple :

```
SHA1 Fingerprint=E4:F0:37:9A:32:52:FA:7D:2E:91:BD:12:7A:2F:A3:75:F8:A1:7B:C4
```

- 3 Copiez l'UID de l'empreinte digitale. Pour la validation, vous devrez éventuellement retirer les deux-points.

Suivant

Conservez l'empreinte digitale que vous avez copiée pour l'utiliser avec le programme d'installation de l'agent de gestion.

Télécharger et installer un agent de gestion

Un administrateur télécharge et installe l'agent de gestion sur la machine IaaS de votre déploiement. L'agent de gestion doit être installé sur le serveur IaaS mais ne doit pas nécessairement être installé sur le serveur de la base de données SQL s'il est séparé.

L'agent de gestion enregistre le nœud IaaS dans le dispositif vRealize Automation appliance, automatise l'installation et la gestion des composants IaaS et collecte les informations de télémétrie et d'assistance. L'agent de gestion est exécuté en tant que service Windows sur votre machine IaaS et vous devez posséder les droits d'administration locale pour installer l'agent.

Prérequis

- Effectuez une copie temporaire de l'empreinte digitale du certificat vRealize Automation appliance comme cela est décrit dans la section « [Trouver l'empreinte digitale de certificat SSL pour le service du site de gestion.](#) », page 36.
- Assurez-vous que l'utilisateur du compte de service est un compte de domaine avec privilèges d'administrateur sur les serveurs Windows IaaS.

Procédure

- 1 Ouvrez votre dispositif vRealize Automation appliance en spécifiant une adresse au format suivant dans un navigateur Web, où *vra-va-hostname.domain.name* est le nom de domaine complet de votre vRealize Automation appliance. N'utilisez pas d'adresse d'équilibrage de charge.
`https://vrealize-automation-appliance-FQDN:5480/installer`
- 2 Cliquez sur **programme d'installation d'agent de gestion** pour télécharger le programme d'installation.
- 3 Exécutez le programme d'installation de l'agent de gestion, vCAC-IaaSManagementAgent-Setup.msi.
L'emplacement par défaut est %Program Files(x86)%\VMware\vCAC\Management Agent\
- 4 Cliquez sur **Suivant** sur la page d'accueil.
- 5 Acceptez le contrat de licence d'utilisateur final, puis cliquez sur **Suivant**.
- 6 Fournissez un nouvel emplacement d'installation ou validez l'emplacement par défaut.
- 7 Cliquez sur **Suivant**.
- 8 Indiquez les détails du service du site de gestion pour les champs suivants. et cliquez sur **Suivant**.

Zone de texte	Entrée
adresse de dispositif vRA	<code>https://vrealize-automation-appliance-FQDN:5480</code> Vous devez spécifier le numéro de port.
Nom d'utilisateur racine	L'utilisateur racine du dispositif vRealize Automation appliance.

Zone de texte	Entrée
Mot de passe	Le mot de passe de l'utilisateur racine du dispositif vRealize Automation appliance.
Certificat du serveur du site de gestion	L'empreinte digitale SHA1 du certificat du service du site de gestion. Le service du site de gestion est hébergé sur le dispositif vRealize Automation appliance. Échantillon d'empreinte SHA1 : DFF5FA0886DA2920D227ADF8BC9CDE4EF13EEF78.
Charge	Cliquez sur Charge pour charger l'empreinte digitale par défaut.

VMware vRealize Automation Management Agent Setup

Management Site Service

Specify the VA host for the Management Site Service to use for the agent.

vRA appliance address:

 Specify the scheme and the port (hosted by default on 5480). Example: https://va-address:5...

Root username: Password:

Provide vRealize Automation appliance root user credentials

Management Site Service certificate SHA1 fingerprint:

☒ I confirm the fingerprint matches the Management Site Service SSL certificate

- 9 Cochez la case **Confirmation de correspondance de l'empreinte digitale** après avoir confirmé que l'empreinte digitale affichée correspond à celle du certificat SSL du site de gestion.
Si les empreintes digitales ne correspondent pas, vérifiez que l'adresse indiquée dans la zone de texte **Adresse du dispositif vRA** est correcte.
- 10 Cliquez sur **Suivant**.
- 11 Entrez le nom d'utilisateur et le mot de passe du compte du service.
- 12 Cliquez sur **Suivant**.
- 13 Cliquez sur **Installer**.
- 14 Cliquez sur **Terminer**.
- 15 Répétez ces étapes pour chaque hôte IaaS Windows.

Après avoir installé l'agent de gestion, le serveur Windows est affiché sur la page des conditions préalables d'installation de l'assistant d'installation.

Synchroniser les heures des serveurs

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

Les options de la page Conditions préalables de l'assistant d'installation vous permettent de sélectionner une méthode de synchronisation de l'heure pour vos dispositifs virtuels. Le tableau des hôtes IaaS vous informe des décalages de temps.

Procédure

- 1 Sélectionnez une option dans le menu **Mode de synchronisation de l'heure**.

Option	Action
Utiliser l'heure du serveur	Sélectionnez Utiliser l'heure du serveur dans le menu Mode de synchronisation de l'heure pour utiliser le protocole de temps du réseau. Pour chaque serveur que vous utilisez, entrez l'adresse IP ou le nom d'hôte dans la zone de texte Heure du serveur .
Utiliser l'heure de l'hôte	Sélectionnez Utiliser l'heure de l'hôte dans le menu Mode de synchronisation de l'heure pour utiliser la synchronisation de l'heure VMware Tools. Pour pouvoir utiliser la synchronisation de l'heure VMware Tools, vous devez configurer au préalable les connexions aux serveurs du protocole de temps du réseau.

- 2 Cliquez sur **Modifiez les paramètres d'heure**.
- 3 Cliquez sur **Suivant**.

Suivant

Vérifiez que vos serveurs IaaS sont configurés correctement.

Exécuter l'outil de vérification des conditions préalables

Exécutez l'outil de vérification des conditions préalables pour vérifier que le serveur Windows pour composants IaaS est correctement configuré.

Procédure

- 1 Cliquez sur **Exécuter** sur l'écran de l'Outil de vérification des conditions préalables.
Une fois les vérifications effectuées, le serveur Windows pour composants IaaS est spécifié avec un état.
- 2 Si un avertissement apparaît, vous pouvez obtenir davantage d'informations sur l'erreur ou choisir de corriger l'erreur automatiquement.
 - ◆ Cliquez sur **Afficher les détails** pour obtenir plus d'informations sur l'erreur et les étapes à suivre pour la corriger.
 - ◆ Cliquez sur **Corriger** pour corriger l'erreur automatiquement.
L'option **Corriger** applique des corrections et redémarre le serveur Windows IaaS.
- 3 Cliquez sur **Exécuter** pour vérifier les corrections.
- 4 Cliquez sur **Suivant** une fois toutes les erreurs corrigées.

Votre serveur Windows est correctement configuré pour l'installation des composants IaaS.

Suivant

Passez à l'écran Hôte vRealize Automation Host.

Spécifier les paramètres d'un déploiement minimal

Utilisez l'assistant d'installation de vRealize Automation pour entrer les paramètres de configuration des composants d'un déploiement minimal.

Prérequis

Procédure

- ◆ Suivez les instructions sur les pages de l'assistant d'installation afin d'entrer les noms de domaines complets des serveurs vRealize Automation appliance et IaaS Windows, les informations d'identification du compte, le mot de passe par défaut du locataire et d'autres paramètres.

L'assistant vérifie que les systèmes respectent les conditions préalables avant de vous laisser entrer les paramètres, et il valide vos paramètres avant de commencer l'installation du produit.

Suivant

Dans vSphere, créez un snapshot de chaque serveur vRealize Automation appliance et Windows IaaS avant de commencer à installer le produit.

Créer des snapshots avant de commencer l'installation

Créez des snapshots de tous vos dispositifs et serveurs Windows. Si l'installation échoue, vous pouvez revenir à ces snapshots et refaire une tentative d'installation.

Les snapshots conservent votre travail de configuration. Veillez à inclure un snapshot du dispositif vRealize Automation appliance sur lequel vous exécutez l'assistant.

Des instructions sont fournies pour les utilisateurs vSphere.

REMARQUE Ne quittez pas l'assistant d'installation et n'annulez pas l'installation.

Procédure

- 1 Ouvrez un autre navigateur et connectez-vous à vSphere Client.
- 2 Localisez votre serveur ou dispositif dans l'inventaire vSphere Client.
- 3 Cliquez avec le bouton droit sur le serveur dans l'inventaire et sélectionnez **Créer un snapshot**.
- 4 Entrez un nom de snapshot.
- 5 Cocher la case **Prendre un snapshot de la mémoire de la machine virtuelle** pour capturer la mémoire du serveur, puis cliquez sur **OK**.

Le snapshot est créé.

Répétez ces étapes pour réaliser des snapshots de tous vos serveurs ou dispositifs.

Suivant

« [Terminer l'installation](#) », page 62

Scénario : terminer l'installation

En tant qu'administrateur vSphere, vous vous trouvez dans la dernière partie de la procédure d'installation. Vous lancez l'installation de vRealize Automation et attendez que celle-ci se termine avec succès.

Procédure

- 1 Revenez à l'assistant d'installation.

- 2 Vérifiez le résumé de l'installation et cliquez sur **Suivant**.
- 3 Saisissez la clé de licence de produit, puis cliquez sur **Suivant**.
- 4 Acceptez ou modifiez les paramètres de télémétrie par défaut et cliquez sur **Suivant**.
- 5 Cliquez sur **Suivant**.
- 6 Cliquez sur **Terminer**.

L'installation démarre. En fonction de votre configuration réseau, l'installation peut prendre entre quinze minutes et une heure.

Un message de confirmation s'affiche une fois l'installation terminée.

Suivant

Vous êtes désormais prêt à configurer votre déploiement.

Échecs de l'installation d'adresse

Lorsque vous réalisez une installation depuis la page Détails d'installation, vous êtes informé de tout problème empêchant l'installation de se terminer.

Lorsque des problèmes se produisent, le composant est signalé et des informations détaillées concernant l'échec, accompagnées d'une marche à suivre pour trouver des solutions, s'affichent. Une fois le problème résolu, vous pouvez réessayer de procéder à l'installation. La marche à suivre pour trouver une solution varie selon le type de problème.

Procédure

- 1 Si le bouton **Réessayer élément échoué** est activé, suivez les étapes suivantes.
 - a Passez l'échec en revue.
 - b Évaluez les modifications à apporter et procédez aux changements requis.
 - c Revenez à l'écran d'installation et cliquez sur **Réessayer élément échoué**.
Le programme d'installation tente d'installer l'ensemble des composants défaillants.
- 2 Si le bouton **Réessayer tous les IaaS** est activé, suivez les étapes suivantes.
 - a Passez l'échec en revue.
 - b Évaluez les modifications à apporter.
 - c Faites revenir tous les serveurs IaaS aux snapshots créés antérieurement.
 - d Supprimez la base de données MS SQL si vous utilisez une base de données externe.
 - e Effectuez les changements nécessaires.
 - f Cliquez sur **Réessayer tous les IaaS**.
- 3 Si le problème se situe au niveau des composants du dispositif virtuel, suivez les étapes suivantes.
 - a Passez l'échec en revue.
 - b Évaluez les modifications à apporter.
 - c Faites revenir tous les serveurs aux snapshots, y compris celui depuis lequel vous exécutez l'assistant.
 - d Effectuez les changements nécessaires.

- e Actualisez la page de l'assistant.
 - f Connectez-vous et exécutez une nouvelle fois l'assistant.
- L'assistant s'ouvre à l'étape de pré-installation.

Configurer les informations d'identification pour la configuration de contenu initial

Vous pouvez également démarrer un workflow de contenu initial pour un point de terminaison vSphere.

Le processus utilise un utilisateur local appelé configurationadmin auquel est attribué des droits d'administrateur.

Procédure

- 1 Créez et entrez un mot de passe pour le compte configurationadmin dans la zone de texte **Mot de passe**.
- 2 Saisissez à nouveau le mot de passe dans la zone de texte **Confirmer le mot de passe**. Notez ce mot de passe pour pouvoir l'utiliser ultérieurement.
- 3 Cliquez sur **Créer le contenu initial**.
- 4 Cliquez sur **Suivant**.

Un utilisateur administrateur de configuration est créé et un élément du catalogue de configuration est créé dans le locataire par défaut. Les droits suivants sont attribués à l'administrateur de configuration :

- Administrateur d'approbations
- Administrateur du catalogue
- Administrateur IaaS
- Architecte d'infrastructure
- Administrateur de locataire
- Architecte XaaS

Suivant

- Lorsque l'assistant se termine, vous pouvez vous connecter au locataire par défaut en tant qu'utilisateur configurationadmin et demander les éléments du catalogue de contenu initial. Pour obtenir un exemple de demande d'élément et d'exécution d'action manuelle d'utilisateur, reportez-vous au document *Installation et configuration de vRealize Automation pour le scénario Rainpole*.
- Configurez l'accès au locataire par défaut pour d'autres utilisateurs. Reportez-vous à « [Configurer l'accès au locataire par défaut](#) », page 125.

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 appliance font échouer l'installation. Une seule instance de serveur Web et vRealize Automation appliance doivent être actives lors de l'installation.

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

Les déploiements d'entreprise sont utilisés pour un environnement de production. Vous pouvez utiliser l'assistant d'installation pour déployer une installation distribuée ou une installation distribuée avec équilibrages de charge pour la haute disponibilité et le basculement.

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.

Prérequis

- Vérifiez que toutes les conditions préalables décrites dans [Chapitre 2, « Préparation à l'installation de vRealize Automation »](#), page 19 sont satisfaites.
- [« Déployer le dispositif vRealize Automation »](#), page 68.

Procédure

- 1 Ouvrez-le vRealize Automation appliance dans un navigateur Web. Utilisez le nom de domaine complet (FQDN).
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Connectez-vous en tant que racine et utilisez le mot de passe que vous avez créé lors du déploiement d'OVA.

Lors de votre première connexion, l'assistant d'installation s'affiche.
- 3 Acceptez le contrat de licence d'utilisateur final.
- 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 Windows IaaS et installez l'agent de gestion. L'agent de gestion permet à l'assistant de détecter ces serveurs IaaS et de s'y connecter.

Suivant

Reportez-vous à [« Installation de l'agent de gestion »](#), page 43.

Installation de l'agent de gestion

Vous devez installer un agent de gestion sur chaque machine Windows hébergeant des composants IaaS.

Si votre dispositif vRealize Automation principal échoue, vous devez réinstaller des agents de gestion.

Les agents de gestion ne sont pas automatiquement supprimés lorsque vous désinstallez un composant IaaS. Désinstallez l'agent de gestion de la même manière que vous désinstalleriez un programme Windows au moyen de l'outil Ajouter ou supprimer des programmes.

Trouver l'empreinte digitale de certificat SSL pour le service du site de gestion.

Lorsque vous installez un agent de gestion, vous devez valider l'empreinte digitale du certificat SSL pour le service du site de gestion.

Vous pouvez obtenir l'empreinte digitale à l'invite de commandes sur vRealize Automation appliance.

Procédure

- 1 Connectez-vous à la console vRealize Automation appliance en tant que racine.
- 2 Entrez la commande suivante :


```
openssl x509 -in /opt/vmware/etc/lighttpd/server.pem -fingerprint -noout -sha1
```

 L'empreinte digitale SHA1 s'affiche. Par exemple :


```
SHA1 Fingerprint=E4:F0:37:9A:32:52:FA:7D:2E:91:BD:12:7A:2F:A3:75:F8:A1:7B:C4
```
- 3 Copiez l'UID de l'empreinte digitale. Pour la validation, vous devrez éventuellement retirer les deux-points.

Suivant

Conservez l'empreinte digitale que vous avez copiée pour l'utiliser avec le programme d'installation de l'agent de gestion.

Télécharger et installer un agent de gestion

Un administrateur télécharge et installe un agent de gestion sur les machines IaaS de votre déploiement. L'agent de gestion doit être installé sur tous les serveurs IaaS exceptés ceux exclusivement utilisés pour votre base de données MS SQL.

L'agent de gestion enregistre les nœuds IaaS avec le dispositif vRealize Automation appliance, automatise l'installation et la gestion des composants IaaS et rassemble les informations de télémétrie et d'assistance. L'agent de gestion est exécuté en tant que service Windows sur votre machine IaaS et vous devez posséder les droits d'administration locale pour installer l'agent.

Prérequis

- Effectuez une copie temporaire de l'empreinte digitale du certificat vRealize Automation appliance comme cela est décrit dans la section « [Trouver l'empreinte digitale de certificat SSL pour le service du site de gestion.](#) », page 36.
- Assurez-vous que l'utilisateur du compte de service est un compte de domaine avec privilèges d'administrateur sur les serveurs Windows IaaS.

Procédure

- 1 Ouvrez votre dispositif vRealize Automation appliance en spécifiant une adresse au format suivant dans un navigateur Web, où *vra-va-hostname.domain.name* est le nom de domaine complet de votre vRealize Automation appliance. N'utilisez pas d'adresse d'équilibrage de charge.


```
https://vrealize-automation-appliance-FQDN:5480/installer
```
- 2 Cliquez sur **programme d'installation d'agent de gestion** pour télécharger le programme d'installation.
- 3 Exécutez le programme d'installation de l'agent de gestion, vCAC-IaaSManagementAgent-Setup.msi.

 L'emplacement par défaut est %Program Files(x86)%\VMware\vCAC\Management Agent\
- 4 Cliquez sur **Suivant** sur la page d'accueil.
- 5 Acceptez le contrat de licence d'utilisateur final, puis cliquez sur **Suivant**.
- 6 Fournissez un nouvel emplacement d'installation ou validez l'emplacement par défaut.
- 7 Cliquez sur **Suivant**.

- 8 Indiquez les détails du service du site de gestion pour les champs suivants, et cliquez sur **Suivant**.

Zone de texte	Entrée
adresse de dispositif vRA	https://vrealize-automation-appliance-FQDN:5480 Vous devez spécifier le numéro de port.
Nom d'utilisateur racine	L'utilisateur racine du dispositif vRealize Automation appliance.
Mot de passe	Le mot de passe de l'utilisateur racine du dispositif vRealize Automation appliance.
Certificat du serveur du site de gestion	L'empreinte digitale SHA1 du certificat du service du site de gestion. Le service du site de gestion est hébergé sur le dispositif vRealize Automation appliance. Échantillon d'empreinte SHA1 : DFF5FA0886DA2920D227ADF8BC9CDE4EF13EEF78.
Charge	Cliquez sur Charge pour charger l'empreinte digitale par défaut.

VMware vRealize Automation Management Agent Setup

Management Site Service

Specify the VA host for the Management Site Service to use for the agent.

vRA appliance address:

 Specify the scheme and the port (hosted by default on 5480). Example: https://va-address:5...

Root username: Password:

Provide vRealize Automation appliance root user credentials

Management Site Service certificate SHA1 fingerprint:

☒ I confirm the fingerprint matches the Management Site Service SSL certificate

- 9 Cochez la case **Confirmation de correspondance de l'empreinte digitale** après avoir confirmé que l'empreinte digitale affichée correspond à celle du certificat SSL du site de gestion.
- Si les empreintes digitales ne correspondent pas, vérifiez que l'adresse indiquée dans la zone de texte **Adresse du dispositif vRA** est correcte.
- 10 Cliquez sur **Suivant**.
- 11 Entrez le nom d'utilisateur et le mot de passe du compte du service.
- 12 Cliquez sur **Suivant**.
- 13 Cliquez sur **Installer**.
- 14 Cliquez sur **Terminer**.
- 15 Répétez ces étapes pour chaque hôte IaaS Windows.

Après avoir installé l'agent de gestion, le serveur Windows est affiché sur la page des conditions préalables d'installation de l'assistant d'installation.

Synchroniser les heures des serveurs

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

Les options de la page Conditions préalables de l'assistant d'installation vous permettent de sélectionner une méthode de synchronisation de l'heure pour vos dispositifs virtuels. Le tableau des hôtes IaaS vous informe des décalages de temps.

Procédure

- 1 Sélectionnez une option dans le menu **Mode de synchronisation de l'heure**.

Option	Action
Utiliser l'heure du serveur	Sélectionnez Utiliser l'heure du serveur dans le menu Mode de synchronisation de l'heure pour utiliser le protocole de temps du réseau. Pour chaque serveur que vous utilisez, entrez l'adresse IP ou le nom d'hôte dans la zone de texte Heure du serveur .
Utiliser l'heure de l'hôte	Sélectionnez Utiliser l'heure de l'hôte dans le menu Mode de synchronisation de l'heure pour utiliser la synchronisation de l'heure VMware Tools. Pour pouvoir utiliser la synchronisation de l'heure VMware Tools, vous devez configurer au préalable les connexions aux serveurs du protocole de temps du réseau.

- 2 Cliquez sur **Modifiez les paramètres d'heure**.
- 3 Cliquez sur **Suivant**.

Suivant

Vérifiez que vos serveurs IaaS sont configurés correctement.

Exécuter l'outil de vérification des conditions préalables

Exécutez l'outil de vérification des conditions préalables pour vérifier que les serveurs Windows pour composants IaaS sont correctement configurés.

Procédure

- 1 Cliquez sur **Exécuter** sur l'écran de l'Outil de vérification des conditions préalables.
Une fois les vérifications effectuées, chaque serveur Windows pour composants IaaS est spécifié avec un état.
- 2 Si un avertissement apparaît, vous pouvez obtenir davantage d'informations sur l'erreur ou choisir de corriger l'erreur automatiquement.
 - ◆ Cliquez sur **Afficher les détails** pour obtenir plus d'informations sur l'erreur et les étapes à suivre pour la corriger.
 - ◆ Cliquez sur **Corriger** pour corriger l'erreur automatiquement.
L'option **Corriger** applique des corrections et redémarre toutes les machines IaaS, notamment celles qui peuvent ne pas avoir de corrections.
- 3 Cliquez sur **Exécuter** pour vérifier les corrections.
- 4 Cliquez sur **Suivant** une fois toutes les erreurs corrigées.

Vos serveurs Windows sont correctement configurés pour l'installation des composants IaaS.

Suivant

Passez à l'écran Hôte vRealize Automation Host.

Spécifier les paramètres d'un déploiement d'entreprise

Utilisez l'assistant d'installation de vRealize Automation pour entrer les paramètres de configuration des composants du déploiement d'entreprise.

Prérequis**Procédure**

- ◆ Suivez les instructions sur les pages de l'assistant d'installation afin d'entrer les noms de domaines complets des serveurs vRealize Automation appliance et IaaS Windows, les informations d'identification du compte, le mot de passe par défaut du locataire et d'autres paramètres.

L'assistant vérifie que les systèmes respectent les conditions préalables avant de vous laisser entrer les paramètres, et il valide vos paramètres avant de commencer l'installation du produit.

Suivant

Dans vSphere, créez un snapshot de chaque serveur vRealize Automation appliance et Windows IaaS avant de commencer à installer le produit.

Créer des snapshots avant de commencer l'installation

Créez des snapshots de tous vos dispositifs et serveurs Windows. Si l'installation échoue, vous pouvez revenir à ces snapshots et refaire une tentative d'installation.

Les snapshots conservent votre travail de configuration. Veillez à inclure un snapshot du dispositif vRealize Automation appliance sur lequel vous exécutez l'assistant.

Des instructions sont fournies pour les utilisateurs vSphere.

REMARQUE Ne quittez pas l'assistant d'installation et n'annulez pas l'installation.

Procédure

- 1 Ouvrez un autre navigateur et connectez-vous à vSphere Client.
- 2 Localisez votre serveur ou dispositif dans l'inventaire vSphere Client.
- 3 Cliquez avec le bouton droit sur le serveur dans l'inventaire et sélectionnez **Créer un snapshot**.
- 4 Entrez un nom de snapshot.
- 5 Cocher la case **Prendre un snapshot de la mémoire de la machine virtuelle** pour capturer la mémoire du serveur, puis cliquez sur **OK**.

Le snapshot est créé.

Répétez ces étapes pour réaliser des snapshots de tous vos serveurs ou dispositifs.

Suivant

« [Terminer l'installation](#) », page 62

Terminer l'installation

Après avoir créé des snapshots, vous lancez l'installation de vRealize Automation et attendez que celle-ci se termine avec succès.

Procédure

- 1 Revenez à l'assistant d'installation.
- 2 Vérifiez le résumé de l'installation et cliquez sur **Suivant**.
- 3 Cliquez sur **Suivant**.
- 4 Cliquez sur **Terminer**.

L'installation démarre. En fonction de votre configuration réseau, l'installation peut prendre entre quinze minutes et une heure.

Un message de confirmation s'affiche une fois l'installation terminée.

Suivant

Vous êtes désormais prêt à configurer votre déploiement.

Échecs de l'installation d'adresse

Lorsque vous réalisez une installation depuis la page Détails d'installation, vous êtes informé de tout problème empêchant l'installation de se terminer.

Lorsque des problèmes se produisent, le composant est signalé et des informations détaillées concernant l'échec, accompagnées d'une marche à suivre pour trouver des solutions, s'affichent. Une fois le problème résolu, vous pouvez réessayer de procéder à l'installation. La marche à suivre pour trouver une solution varie selon le type de problème.

Procédure

- 1 Si le bouton **Réessayer élément échoué** est activé, suivez les étapes suivantes.
 - a Passez l'échec en revue.
 - b Évaluez les modifications à apporter et procédez aux changements requis.
 - c Revenez à l'écran d'installation et cliquez sur **Réessayer élément échoué**.
Le programme d'installation tente d'installer l'ensemble des composants défaillants.
- 2 Si le bouton **Réessayer tous les IaaS** est activé, suivez les étapes suivantes.
 - a Passez l'échec en revue.
 - b Évaluez les modifications à apporter.
 - c Faites revenir tous les serveurs IaaS aux snapshots créés antérieurement.
 - d Supprimez la base de données MS SQL si vous utilisez une base de données externe.
 - e Effectuez les changements nécessaires.
 - f Cliquez sur **Réessayer tous les IaaS**.
- 3 Si le problème se situe au niveau des composants du dispositif virtuel, suivez les étapes suivantes.
 - a Passez l'échec en revue.
 - b Évaluez les modifications à apporter.

- c Faites revenir tous les serveurs aux snapshots, y compris celui depuis lequel vous exécutez l'assistant.
- d Effectuez les changements nécessaires.
- e Actualisez la page de l'assistant.
- f Connectez-vous et exécutez une nouvelle fois l'assistant.

L'assistant s'ouvre à l'étape de pré-installation.

Configurer les informations d'identification pour la configuration de contenu initial

Vous pouvez également démarrer un workflow de contenu initial pour un point de terminaison vSphere.

Le processus utilise un utilisateur local appelé configurationadmin auquel est attribué des droits d'administrateur.

Procédure

- 1 Créez et entrez un mot de passe pour le compte configurationadmin dans la zone de texte **Mot de passe**.
- 2 Saisissez à nouveau le mot de passe dans la zone de texte **Confirmer le mot de passe**. Notez ce mot de passe pour pouvoir l'utiliser ultérieurement.
- 3 Cliquez sur **Créer le contenu initial**.
- 4 Cliquez sur **Suivant**.

Un utilisateur administrateur de configuration est créé et un élément du catalogue de configuration est créé dans le locataire par défaut. Les droits suivants sont attribués à l'administrateur de configuration :

- Administrateur d'approbations
- Administrateur du catalogue
- Administrateur IaaS
- Architecte d'infrastructure
- Administrateur de locataire
- Architecte XaaS

Suivant

- Lorsque l'assistant se termine, vous pouvez vous connecter au locataire par défaut en tant qu'utilisateur configurationadmin et demander les éléments du catalogue de contenu initial. Pour obtenir un exemple de demande d'élément et d'exécution d'action manuelle d'utilisateur, reportez-vous au document *Installation et configuration de vRealize Automation pour le scénario Rainpole*.
- Configurez l'accès au locataire par défaut pour d'autres utilisateurs. Reportez-vous à « [Configurer l'accès au locataire par défaut](#) », page 125.

Les interfaces d'installation standard de vRealize Automation

4

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 3, « Installation de vRealize Automation avec l'assistant Installation »](#), page 33 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.
- L'installation au moyen de l'assistant échoue pour une raison quelconque.
- Vous souhaitez ajouter un autre dispositif vRealize Automation appliance 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 aborde les rubriques suivantes :

- [« Utilisation des interfaces standard pour des déploiements minimaux »](#), page 51
- [« Utilisation des interfaces standard pour les déploiements distribués »](#), page 63
- [« Installation d'agents vRealize Automation »](#), page 102

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

Un administrateur système peut déployer un dispositif vRealize Automation complet dans une configuration minimale. En général, les déploiements minimaux sont utilisés dans un environnement de développement ou en tant que validation technique et nécessitent une procédure d'installation plus courte.

La Liste de contrôle pour un déploiement minimal fournit une présentation de haut niveau sur la séquence des tâches à réaliser pour effectuer une installation minimale.

Imprimez une copie de la liste de contrôle et utilisez-la pour le suivi de votre travail au fur et à mesure de l'installation. Effectuez les tâches dans l'ordre dans lequel elles sont fournies.

Tableau 4-1. Liste de contrôle pour un déploiement minimal

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 », page 19
<input type="checkbox"/> Configurez votre dispositif vRealize Automation appliance	« Déployer et configurer le dispositif vRealize Automation », page 52
<input type="checkbox"/> Installez les composants IaaS sur un seul serveur Windows.	« Installation des composants IaaS », page 57
<input type="checkbox"/> Installez des agents supplémentaires, au besoin.	« Installation d'agents vRealize Automation », page 102
<input type="checkbox"/> Effectuez des tâches de post-installation comme la configuration du locataire par défaut.	

Déployer et configurer le dispositif vRealize Automation

Le dispositif vRealize Automation appliance est un dispositif virtuel préconfiguré qui déploie le serveur vRealize Automation appliance et la console Web (le portail utilisateur). Il est fourni sous la forme d'un modèle de format de virtualisation ouvert (OVF). L'administrateur système télécharge le dispositif et le déploie dans l'inventaire vCenter Server ou ESX/ESXi.

- 1 [Déployer le dispositif vRealize Automation](#) page 52
Pour déployer le dispositif vRealize Automation appliance, un administrateur système doit se connecter au client vSphere et sélectionner les paramètres de déploiement.
- 2 [Activer la synchronisation de l'heure sur le dispositif vRealize Automation](#) page 54
Les horloges sur le serveur vRealize Automation et les serveurs Windows doivent être synchronisées pour que l'installation réussisse.
- 3 [Configurer le dispositif vRealize Automation](#) page 55
Pour préparer le dispositif vRealize Automation appliance, un administrateur système configure les paramètres de l'hôte, génère un certificat SSL et fournit les informations de connexion de SSO.

Déployer le dispositif vRealize Automation

Pour déployer le dispositif vRealize Automation appliance, un administrateur système doit se connecter au client vSphere et sélectionner les paramètres de déploiement.

Certaines restrictions s'appliquent au mot de passe racine que vous avez créé pour l'administrateur de vRealize Automation.

Prérequis

- Téléchargez le dispositif vRealize Automation appliance sur le site Web VMware.

- Connectez-vous au client vSphere en tant qu'utilisateur disposant des privilèges d'administrateur système.

Procédure

- 1 Sélectionnez **Fichier > Déployer un modèle OVF** depuis le client vSphere.
- 2 Accédez au fichier vRealize Automation appliance que vous avez téléchargé et cliquez sur **Ouvrir**.
- 3 Cliquez sur **Suivant**.
- 4 Sur la page des détails du modèle OVF, cliquez sur **Suivant**.
- 5 Acceptez le contrat de licence, puis cliquez sur **Suivant**.
- 6 Entrez un nom de dispositif virtuel unique conformément à la convention d'affectation de noms de votre organisation dans la zone de texte **Nom**, sélectionnez le centre de données et l'emplacement dans lequel vous souhaitez déployer le dispositif virtuel et cliquez sur **Suivant**.
- 7 Suivez les invites jusqu'à ce que la page Format de disque apparaisse.
- 8 Sur la page Format de disque, vérifiez que l'espace est suffisant pour déployer le dispositif virtuel et cliquez sur **Suivant**.
- 9 Suivez les invites jusqu'à la page Propriétés.
Les options qui apparaissent dépendent de votre configuration vSphere.
- 10 Configurez les valeurs sur la page Propriétés.
 - a Entrez le mot de passe racine qui doit être utilisé pour se connecter à la console du dispositif virtuel dans les zones de texte **Entrer le mot de passe** et **Confirmer le mot de passe**.
 - b Cochez ou décochez la case **Service SSH** pour choisir si le service SSH est activé ou non pour le dispositif.

Cette valeur permet de définir le statut initial du service SSH dans le dispositif. Si vous installez l'assistant d'installation, activez cette option avant de l'exécuter. Vous pouvez modifier ce paramètre depuis la console de gestion du dispositif après l'installation.
 - c Entrez le nom de domaine complet de la machine virtuelle dans la zone de texte **Nom d'hôte**.
 - d Configurez les propriétés du réseau.
- 11 Cliquez sur **Suivant**.
- 12 Selon votre déploiement, vCenter, et la configuration de DNS, sélectionnez l'une des manières suivantes de terminer le déploiement OVA et la mise sous tension de vRealize Automation appliance.
 - 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 le déploiement des fichiers effectué dans vCenter, cliquez sur **Fermé**.
 - c Attendez le démarrage de la machine, qui peut durer 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 le déploiement des fichiers effectué dans vCenter, cliquez sur **Fermé**.
 - b Mettez sous-tension le dispositif vRealize Automation appliance.
 - c Attendez le démarrage de la machine, qui peut durer jusqu'à 5 minutes.
 - d Vérifiez que vous pouvez effectuer un test ping sur le serveur DNS du dispositif vRealize Automation appliance. Dans le cas contraire, redémarrez la machine virtuelle.

- e Attendez le démarrage de la machine, qui peut durer jusqu'à 5 minutes.
- Si vous avez déployé le dispositif vRealize Automation appliance 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 appliance.
 - b Cliquez avec le bouton droit sur le dispositif vRealize Automation appliance, 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 appliance.
 - f Attendez le démarrage de la machine, qui peut durer jusqu'à 5 minutes.
- 13 Ouvrez une invite de commande et effectuez un test ping sur le nom de domaine complet pour vérifier que celui-ci peut être résolu sur l'adresse IP de vRealize Automation appliance.

Activer la synchronisation de l'heure sur le dispositif vRealize Automation

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

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

Prérequis

« Déployer le dispositif vRealize Automation », page 33.

Procédure

- 1 Accédez à la console de gestion de vRealize Automation appliance en utilisant son nom de domaine complet (`https://vra-va-hostname.domain.name:5480/`).
- 2 Connectez-vous à l'aide du nom d'utilisateur **racine** et du mot de passe que vous avez spécifiés lorsque le dispositif a été déployé.
- 3 Sélectionnez **Admin > Paramètres d'heure**.
- 4 Sélectionnez une option dans le menu **Mode de synchronisation de l'heure**.

Option	Action
Utiliser l'heure du serveur	Sélectionnez Utiliser l'heure du serveur dans le menu Mode de synchronisation de l'heure pour utiliser le protocole de temps du réseau. Pour chaque serveur que vous utilisez, entrez l'adresse IP ou le nom d'hôte dans la zone de texte Heure du serveur .
Utiliser l'heure de l'hôte	Sélectionnez Utiliser l'heure de l'hôte dans le menu Mode de synchronisation de l'heure pour utiliser la synchronisation de l'heure VMware Tools. Pour pouvoir utiliser la synchronisation de l'heure VMware Tools, vous devez configurer au préalable les connexions aux serveurs du protocole de temps du réseau.

- 5 Cliquez sur **Enregistrer les paramètres**.
- 6 Cliquez sur **Actualiser**.

- 7 Vérifiez que la valeur affichée dans **Heure actuelle** est correcte.
Vous pouvez modifier le fuseau horaire selon les besoins depuis la page Paramètres de fuseau horaire dans l'onglet **Système**.
- 8 (Facultatif) Cliquez sur **Fuseau horaire** dans l'onglet **Système** et sélectionnez un fuseau horaire parmi les choix du menu.
La valeur par défaut est Etc/UTC.
- 9 Cliquez sur **Enregistrer les paramètres**.

Configurer le dispositif vRealize Automation

Pour préparer le dispositif vRealize Automation appliance, un administrateur système configure les paramètres de l'hôte, génère un certificat SSL et fournit les informations de connexion de SSO.

Prérequis

« [Activer la synchronisation de l'heure sur le dispositif vRealize Automation](#) », page 54.

Procédure

- 1 Accédez à la console de gestion de vRealize Automation appliance en utilisant son nom de domaine complet (<https://vra-va-hostname.domain.name:5480/>).
- 2 Continuez après l'avertissement de certificat.
- 3 Connectez-vous avec le nom root et le mot de passe que vous avez spécifié lorsque vous avez déployé le dispositif vRealize Automation appliance.
- 4 Sélectionnez **Paramètres vRA > Paramètres de l'hôte**.

Option	Action
Résoudre automatiquement	Sélectionnez Résoudre automatiquement pour spécifier le nom de l'hôte actuel du dispositif vRealize Automation appliance.
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 appliance, <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>

REMARQUE 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 le type de certificat 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 vRealize Automation appliance et à tous les équilibres de charge par le biais de l'utilisation de certificats SAN (autre nom de l'objet).

REMARQUE 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 appliance 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.
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. REMARQUE Dans le cas de certificats en chaînes, des attributs supplémentaires peuvent être disponibles. 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.

REMARQUE 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 **Paramètres 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**.

REMARQUE 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 la console vRealize Automation.
 - a Ouvrez un navigateur et accédez à `https://vcac-hostname.domain.name/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.

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

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

Suivant

[« Installer les composants d'infrastructure », page 58](#)

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](#) », page 79 dans le chapitre consacré au déploiement distribué.

Installer les composants d'infrastructure

L'administrateur système se connecte à la machine Windows et suit l'assistant d'installation pour installer les composants de l'infrastructure (IaaS) sur la machine virtuelle ou physique Windows.

Prérequis

- Vérifiez que la machine d'installation remplit les conditions requises décrites dans « [Exigences relatives au service Web IaaS et au serveur Model Manager](#) », page 22.
- « [Activer la synchronisation de l'heure sur le serveur Windows](#) », page 57.
- Vérifiez que vous avez déployé et configuré entièrement le dispositif vRealize Automation appliance, 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 Automation IaaS](#) page 59
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 appliance.
- 2 [Sélectionner le type d'installation](#) page 59
L'administrateur système exécute l'assistant du programme d'installation sur la machine d'installation Windows 2008 ou 2012.
- 3 [Vérifier les conditions préalables](#) page 60
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](#) page 60
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](#) page 61
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](#) page 62

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

7 [Terminer l'installation](#) page 62

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

Télécharger le programme d'installation de vRealize Automation IaaS

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 appliance.

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

Prérequis

- Microsoft .NET Framework 4.5.2 ou version ultérieure. Vous pouvez télécharger le programme d'installation de .NET à partir de la même page Web que le programme d'installation d'IaaS.
- Si vous utilisez Internet Explorer pour le téléchargement, vérifiez que l'option de configuration de sécurité renforcée n'est pas activée. Pointez Internet Explorer sur `res://iesetup.dll/SoftAdmin.htm` sur le serveur Windows.

Procédure

- 1 À l'aide d'un compte disposant de privilèges d'administrateur, connectez-vous au serveur Windows.
- 2 Pointez un navigateur Web sur l'URL suivante dans le dispositif vRealize Automation appliance.
`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 appliance

Sélectionner le type d'installation

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

Prérequis

« [Télécharger le programme d'installation de vRealize Automation IaaS](#) », page 79.

Procédure

- 1 Cliquez avec le bouton droit sur le fichier d'installation `setup__vra-va-hostname.domain.name@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 appliance 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 de vRealize Automation appliance.
 - 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 appliance. Vous pouvez afficher le certificat vRealize Automation appliance dans le navigateur du client si vous avez accédé à la console 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.

Prérequis

« [Sélectionner le type d'installation](#) », page 59.

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**.

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.

Prérequis

« [Vérifier les conditions préalables](#) », page 60.

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.

REMARQUE 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 en savoir plus sur la configuration de SSL sur le serveur SQL, reportez-vous à [l'article 316898 de la base de connaissances de Microsoft](#).

- 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.

Prérequis

« [Spécifier les paramètres de serveur et de compte](#) », page 60.

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.

Prérequis

« [Télécharger le programme d'installation de vRealize Automation IaaS](#) », page 59.

Procédure

- 1 Acceptez la valeur **Serveur** par défaut, qui est renseignée avec le nom de domaine complet du serveur vRealize Automation appliance sur lequel 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 extraire le certificat de vRealize Automation appliance.

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'IaaS.

Prérequis

- « [Enregistrer les composants IaaS](#) », page 62.
- 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 appliance à partir duquel vous téléchargez le programme d'installation d'IaaS.

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**.

L'installation est maintenant terminée.

Suivant

« Vérifier les services IaaS », page 101.

Utilisation des interfaces standard pour les déploiements distribués

Dans un déploiement d'entreprise distribué, l'administrateur système installe les composants sur plusieurs machines dans l'environnement de déploiement.

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 4-2. 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 », page 19
<input type="checkbox"/> Planifiez et obtenez vos certificats SSL.	« Exigences d'approbation de certificat dans un déploiement distribué », page 65
<input type="checkbox"/> Déployez le serveur vRealize Automation appliance principal, et tous les dispositifs supplémentaires nécessaires pour la redondance et la haute disponibilité.	« Déployer le dispositif vRealize Automation », page 68
<input type="checkbox"/> Configurez votre équilibrage de charge pour gérer le trafic des dispositifs vRealize Automation.	« Configuration de votre équilibrage de charge », page 70
<input type="checkbox"/> Configurez le serveur vRealize Automation appliance principal, et tous les dispositifs supplémentaires que vous avez déployés pour la redondance et la haute disponibilité.	« Configuration de dispositifs pour vRealize Automation », page 70
<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 », page 77
<input type="checkbox"/> Le cas échéant, installez les agents pour l'intégration à des systèmes externes.	« Installation d'agents vRealize Automation », page 102
<input type="checkbox"/> Configurez le locataire par défaut et fournissez la licence IaaS.	« Configurer l'accès au locataire par défaut », page 125

vRealize Orchestrator

vRealize Automation appliance 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*.

Composants d'une installation distribuée

Dans une installation distribuée, l'administrateur système déploie les dispositifs et les composants associés pour prendre en charge l'environnement de déploiement.

Tableau 4-3. Dispositifs virtuels et base de données de dispositif

Composant	Description
vRealize Automation appliance	Dispositif virtuel préconfiguré qui déploie le serveur vRealize Automation. Le serveur inclut la console du dispositif vRealize Automation, qui fournit un portail unique pour le provisionnement en libre-service et la gestion des services cloud, ainsi que la création et l'administration.
Base de données de dispositif	Stocke les informations requises par les dispositifs virtuels. La base de données est intégrée dans une ou deux instances de vRealize Automation appliance.

Vous pouvez sélectionner les composants IaaS individuels que vous souhaitez installer et spécifier l'emplacement de l'installation.

Tableau 4-4. Composants IaaS

Composant	Description
Site Web	Fournit les fonctionnalités d'administration et de création de service à la console vRealize Automation. Le composant de site Web communique avec Model Manager, qui lui fournit les mises à jour de Distributed Execution Manager (DEM), des agents proxy et de la base de données.
Manager Service	Manager Service coordonne la communication entre les agents, la base de données, Active Directory et SMTP. Manager Service communique avec le site de la console Web par l'intermédiaire de Model Manager. Pour exécuter ce service, des privilèges d'administrateur sont requis.
Model Manager	Model Manager communique avec la base de données, les DEM et le site Web du portail. Model Manager est divisé en deux composants installables séparément : le service Web Model Manager et le composant de données Web Manager.
Instances de Distributed Execution Manager (Orchestrator et travailleur)	Une instance de Distributed Execution Manager (DEM) exécute la logique du système de modèles personnalisés, interagissant avec la base de données IaaS et les bases de données externes. Les instances DEM gèrent également les machines dans le cloud et physiques.
Agents	Agents de virtualisation, d'intégration et WMI qui communiquent avec les ressources de l'infrastructure.

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 appliance 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 de composants vRealize Automation appliance ou 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 appliance et composants IaaS, vous pouvez réactiver les contrôles de santé.

Exigences d'approbation de certificat dans un déploiement distribué

Pour une communication sécurisée, vRealize Automation s'appuie sur des certificats afin de créer des relations de confiance entre les composants.

La mise en œuvre spécifique des certificats requis pour obtenir cette confiance dépend de votre environnement.

Pour assurer la prise en charge de la haute disponibilité et du basculement, vous devez déployer des clusters de composants équilibrés. Dans ce cas, vous obtenez un certificat polyvalent qui inclut le composant Web IaaS du cluster, puis vous copiez ce certificat polyvalent dans chaque composant du cluster. Vous pouvez utiliser des certificats SAN (Subject Alternative Name), des certificats génériques ou toute autre méthode de certification réutilisable adaptée à votre environnement, tant que vous respectez les conditions requises en matière d'approbation. Si vous utilisez des équilibres de charge dans votre déploiement, vous devez inclure le nom de domaine complet de l'équilibrage de charge dans l'adresse approuvée du certificat polyvalent du cluster.

Par exemple, si la configuration de votre équilibrage de charge requiert un certificat sur l'équilibrage de charge ainsi que sur ses composants, vous pouvez obtenir un certificat SAN pour certifier `web-load-balancer.eng.mycompany.com`, `web-component-1.eng.mycompany.com` et `web-component-2.eng.mycompany.com`. Vous devez copier ce certificat polyvalent unique sur l'équilibrage de charge et sur chacun de ses dispositifs, puis enregistrer ce certificat sur les machines des composants Web.

Le tableau Exigences d'approbation de certificat récapitule les conditions d'enregistrement de confiance pour les divers certificats importés.

Tableau 4-5. Exigences d'approbation de certificat

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

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.

Prérequis

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.

REMARQUE 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.

Suivant

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

Vous pouvez utiliser ces feuilles d'activité pour enregistrer les informations importantes à des fins de référence lors du processus d'installation.

Une copie de chaque feuille d'activité est fournie ici. Créez des copies supplémentaires selon vos besoins. Les paramètres sont sensibles à la casse.

Tableau 4-6. Informations sur le cluster principal vRealize Automation appliance

Variable	Valeur	Exemple
Nom d'hôte (FQDN)		vcac-va.mycompany.com
IP		192.168.1.105

Tableau 4-6. Informations sur le cluster principal vRealize Automation appliance (suite)

Variable	Valeur	Exemple
Username	administrator@vsphere.local (par défaut)	administrator@vsphere.local
Mot de passe		vmware

Tableau 4-7. Informations vRealize Automation appliance complémentaires

Variable	Valeur	Exemple
Nom d'hôte (FQDN)		vcac-va2.mycompany.com
IP		192.168.1.110
Username	administrator@vsphere.local (par défaut)	administrator@vsphere.local
Mot de passe		vmware

Tableau 4-8. Phrase secrète pour la base de données IaaS

Variable	Valeur	Exemple
Phrase secrète (réutilisée dans le programme d'installation, la mise à niveau et la migration d'IaaS)		myPassphrase

Tableau 4-9. Site Web IaaS

Variable	Valeur	Exemple
Nom d'hôte (FQDN)		iaas-web.mycompany.com
Service SSO sur le port sortant HTTPS (par défaut)		
IP		192.168.1.106
Username		
Mot de passe		

Tableau 4-10. Données IaaS Model Manager

Variable	Valeur	Exemple
Nom d'hôte (FQDN)		iaas-model-man.mycompany.com
Service SSO sur le port sortant HTTPS (par défaut)		
IP		192.168.1.107
Username		
Mot de passe		

Tableau 4-11. IaaS Model Service

Variable	Valeur	Exemple
Nom d'hôte (FQDN)		iaas-model-service.mycompany.com
Service SSO sur le port sortant HTTPS (par défaut)		
IP		192.168.1.108

Tableau 4-11. IaaS Model Service (suite)

Variable	Valeur	Exemple
Username		
Mot de passe		

Tableau 4-12. Instances de Distributed Execution Manager

Nom unique	Orchestrator/Travailleur
ex. myuniqueorchestratorname	Orchestrator : Travailleur :
	Orchestrator : Travailleur :
	Orchestrator : Travailleur :
	Orchestrator : Travailleur :

Déployer le dispositif vRealize Automation

Pour déployer le dispositif vRealize Automation appliance, un administrateur système doit se connecter au client vSphere et sélectionner les paramètres de déploiement.

Certaines restrictions s'appliquent au mot de passe racine que vous avez créé pour l'administrateur de vRealize Automation.

Prérequis

- Téléchargez le dispositif vRealize Automation appliance sur le site Web VMware.
- Connectez-vous au client vSphere en tant qu'utilisateur disposant des privilèges d'administrateur système.

Procédure

- 1 Sélectionnez **Fichier > Déployer un modèle OVF** depuis le client vSphere.
- 2 Accédez au fichier vRealize Automation appliance que vous avez téléchargé et cliquez sur **Ouvrir**.
- 3 Cliquez sur **Suivant**.
- 4 Sur la page des détails du modèle OVF, cliquez sur **Suivant**.
- 5 Acceptez le contrat de licence, puis cliquez sur **Suivant**.
- 6 Entrez un nom de dispositif virtuel unique conformément à la convention d'affectation de noms de votre organisation dans la zone de texte **Nom**, sélectionnez le centre de données et l'emplacement dans lequel vous souhaitez déployer le dispositif virtuel et cliquez sur **Suivant**.
- 7 Suivez les invites jusqu'à ce que la page Format de disque apparaisse.
- 8 Sur la page Format de disque, vérifiez que l'espace est suffisant pour déployer le dispositif virtuel et cliquez sur **Suivant**.
- 9 Suivez les invites jusqu'à la page Propriétés.

Les options qui apparaissent dépendent de votre configuration vSphere.

- 10 Configurez les valeurs sur la page **Propriétés**.
 - a Entrez le mot de passe racine qui doit être utilisé pour se connecter à la console du dispositif virtuel dans les zones de texte **Entrer le mot de passe** et **Confirmer le mot de passe**.
 - b Cochez ou décochez la case **Service SSH** pour choisir si le service SSH est activé ou non pour le dispositif.

 Cette valeur permet de définir le statut initial du service SSH dans le dispositif. Si vous installez l'assistant d'installation, activez cette option avant de l'exécuter. Vous pouvez modifier ce paramètre depuis la console de gestion du dispositif après l'installation.
 - c Entrez le nom de domaine complet de la machine virtuelle dans la zone de texte **Nom d'hôte**.
 - d Configurez les propriétés du réseau.
- 11 Cliquez sur **Suivant**.
- 12 Selon votre déploiement, vCenter, et la configuration de DNS, sélectionnez l'une des manières suivantes de terminer le déploiement OVA et la mise sous tension de vRealize Automation appliance.
 - 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 le déploiement des fichiers effectué dans vCenter, cliquez sur **Fermé**.
 - c Attendez le démarrage de la machine, qui peut durer 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 le déploiement des fichiers effectué dans vCenter, cliquez sur **Fermé**.
 - b Mettez sous-tension le dispositif vRealize Automation appliance.
 - c Attendez le démarrage de la machine, qui peut durer jusqu'à 5 minutes.
 - d Vérifiez que vous pouvez effectuer un test ping sur le serveur DNS du dispositif vRealize Automation appliance. Dans le cas contraire, redémarrez la machine virtuelle.
 - e Attendez le démarrage de la machine, qui peut durer jusqu'à 5 minutes.
 - Si vous avez déployé le dispositif vRealize Automation appliance 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 appliance.
 - b Cliquez avec le bouton droit sur le dispositif vRealize Automation appliance, 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 appliance.
 - f Attendez le démarrage de la machine, qui peut durer jusqu'à 5 minutes.

Pour vérifier si vous avez correctement déployé le dispositif, ouvrez une invite de commande et effectuez un test ping sur le nom de domaine complet du dispositif vRealize Automation appliance.

Suivant

Répétez cette procédure pour déployer d'autres instances du dispositif vRealize Automation appliance à des fins de redondance dans un environnement de haute disponibilité.

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 vRealize Automation appliance.

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 d'approbation de certificat dans un déploiement distribué](#) », page 65. Pour plus d'informations sur l'extraction de certificats, reportez-vous à « [Extraction de certificats et de clés privées](#) », page 31.
- 5 Configurez l'équilibrage de charge pour le trafic vRealize Automation appliance.
- 6 Configurez les dispositifs pour vRealize Automation. Reportez-vous à « [Configuration de dispositifs pour vRealize Automation](#) », page 70.

REMARQUE 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 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.

Configurer le dispositif vRealize Automation principal

Le dispositif vRealize Automation appliance est un dispositif virtuel préconfiguré qui déploie le serveur vRealize Automation et la console Web (le portail utilisateur). Il est fourni sous la forme d'un modèle de format de virtualisation ouvert (OVF). L'administrateur système télécharge le dispositif et le déploie dans l'inventaire vCenter Server ou ESX/ESXi.

Si votre réseau ou votre équilibrage de charge l'exigent, le certificat que vous configurez pour l'instance principale du dispositif est copié dans l'équilibrage de charge et les instances de dispositif supplémentaires dans les procédures suivantes.

Prérequis

- « [Déployer le dispositif vRealize Automation](#) », page 68.
- Obtenez un certificat de domaine pour le dispositif vRealize Automation appliance.

Procédure

- 1 [Activer la synchronisation de l'heure sur le dispositif vRealize Automation appliance](#) page 71
Les horloges sur le serveur vRealize Automation appliance et les serveurs Windows doivent être synchronisées pour que l'installation réussisse.
- 2 [Configurer le dispositif vRealize Automation](#) page 71
Pour préparer le dispositif vRealize Automation appliance, un administrateur système configure les paramètres de l'hôte, génère un certificat SSL et fournit les informations de connexion de SSO.

Activer la synchronisation de l'heure sur le dispositif vRealize Automation appliance

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

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

Procédure

- 1 Accédez à la console de gestion de vRealize Automation appliance en utilisant son nom de domaine complet (<https://vra-va-hostname.domain.name:5480/>).
- 2 Connectez-vous à l'aide du nom d'utilisateur **racine** et du mot de passe que vous avez spécifiés lorsque le dispositif a été déployé.
- 3 Sélectionnez **Admin > Paramètres d'heure**.
- 4 Sélectionnez une option dans le menu **Mode de synchronisation de l'heure**.

Option	Action
Utiliser l'heure du serveur	Sélectionnez Utiliser l'heure du serveur dans le menu Mode de synchronisation de l'heure pour utiliser le protocole de temps du réseau. Pour chaque serveur que vous utilisez, entrez l'adresse IP ou le nom d'hôte dans la zone de texte Heure du serveur .
Utiliser l'heure de l'hôte	Sélectionnez Utiliser l'heure de l'hôte dans le menu Mode de synchronisation de l'heure pour utiliser la synchronisation de l'heure VMware Tools. Pour pouvoir utiliser la synchronisation de l'heure VMware Tools, vous devez configurer au préalable les connexions aux serveurs du protocole de temps du réseau.

- 5 Cliquez sur **Enregistrer les paramètres**.
- 6 Vérifiez que la valeur affichée dans **Heure actuelle** est correcte.

Vous pouvez modifier le fuseau horaire selon les besoins depuis la page Paramètres de fuseau horaire dans l'onglet **Système**.

Configurer le dispositif vRealize Automation

Pour préparer le dispositif vRealize Automation appliance, un administrateur système configure les paramètres de l'hôte, génère un certificat SSL et fournit les informations de connexion de SSO.

Procédure

- 1 Accédez à la console de gestion de vRealize Automation appliance en utilisant son nom de domaine complet (<https://vra-va-hostname.domain.name:5480/>).
- 2 Continuez après l'avertissement de certificat.
- 3 Connectez-vous avec le nom root et le mot de passe que vous avez spécifié lorsque vous avez déployé le dispositif vRealize Automation appliance.

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

Option	Action
Résoudre automatiquement	Sélectionnez Résoudre automatiquement pour spécifier le nom de l'hôte actuel du dispositif vRealize Automation appliance.
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 appliance, <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>

REMARQUE 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 le type de certificat 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 vRealize Automation appliance et à tous les équilibres de charge par le biais de l'utilisation de certificats SAN (autre nom de l'objet).

REMARQUE 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	<ol 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 appliance 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.
Importer	<ol 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. REMARQUE Dans le cas de certificats en chaînes, des attributs supplémentaires peuvent être disponibles. 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 équilibre de charge, copiez le certificat importé ou nouvellement créé sur l'équilibre 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 la console de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.
- 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.

REMARQUE 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 **Paramètres 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**.

REMARQUE 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 la console vRealize Automation.

- a Ouvrez un navigateur et accédez à `https://vcac-hostname.domain.name/vcac`.
Si vous utilisez un équilibrage de charge, le nom d'hôte doit être le nom de domaine complet de l'équilibrage de charge.
- 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.
La console 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 appliance afin d'assurer la redondance dans un environnement de haute disponibilité.

Pour chaque dispositif vRealize Automation appliance, 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 appliance initial (principal) 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.

Activer la synchronisation de l'heure sur le dispositif vRealize Automation Dispositif

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

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

Prérequis

« [Configurer le dispositif vRealize Automation principal](#) », page 70.

Procédure

- 1 Accédez à la console de gestion de vRealize Automation appliance en utilisant son nom de domaine complet (<https://vra-va-hostname.domain.name:5480/>).
- 2 Connectez-vous à l'aide du nom d'utilisateur **racine** et du mot de passe que vous avez spécifiés lorsque le dispositif a été déployé.
- 3 Sélectionnez **Admin > Paramètres d'heure**.
- 4 Sélectionnez une option dans le menu **Mode de synchronisation de l'heure**.

Option	Action
Utiliser l'heure du serveur	Sélectionnez Utiliser l'heure du serveur dans le menu Mode de synchronisation de l'heure pour utiliser le protocole de temps du réseau. Pour chaque serveur que vous utilisez, entrez l'adresse IP ou le nom d'hôte dans la zone de texte Heure du serveur .
Utiliser l'heure de l'hôte	Sélectionnez Utiliser l'heure de l'hôte dans le menu Mode de synchronisation de l'heure pour utiliser la synchronisation de l'heure VMware Tools. Pour pouvoir utiliser la synchronisation de l'heure VMware Tools, vous devez configurer au préalable les connexions aux serveurs du protocole de temps du réseau.

- 5 Cliquez sur **Enregistrer les paramètres**.
- 6 Vérifiez que la valeur affichée dans **Heure actuelle** est correcte.

Vous pouvez modifier le fuseau horaire selon les besoins depuis la page Paramètres de fuseau horaire dans l'onglet **Système**.

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 vRealize Automation appliance.

Vous utilisez la console de gestion sur le nouveau dispositif vRealize Automation appliance 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.

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

Prérequis

- Vous devez déjà disposer d'un ou de plusieurs nœuds vRealize Automation appliance dans le cluster, dont un nœud est le nœud principal. Reportez-vous à « [Configurer le dispositif vRealize Automation principal](#) », page 70.
Vous pouvez désigner un nouveau nœud comme nœud principal uniquement après avoir joint le nouveau nœud au cluster.
- Vérifiez que l'équilibrage de charge est configuré pour une utilisation avec le nouveau dispositif vRealize Automation appliance.
- 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.
- Activez la synchronisation de l'heure sur le nouveau nœud. Reportez-vous à « [Activer la synchronisation de l'heure sur le dispositif vRealize Automation Dispositif](#) », page 75.
- Vérifiez que tous les services vRealize Automation ont démarré, sur les nœuds de dispositifs de cluster existants et sur le nouveau nœud que vous ajoutez.

Procédure

- 1 Accédez à la console de gestion de vRealize Automation appliance en utilisant son nom de domaine complet (<https://vra-va-hostname.domain.name:5480/>).
- 2 Continuez après l'affichage éventuel des avertissements de certificat.
- 3 Connectez-vous avec le nom d'utilisateur racine et le mot de passe que vous avez spécifiés lors du déploiement du dispositif vRealize Automation appliance.
- 4 Sélectionnez **Paramètres vRA > Cluster**.
- 5 Entrez le nom de domaine complet d'un dispositif vRealize Automation appliance configuré précédemment dans la zone de texte **Nœud de cluster de début**.
Vous pouvez utiliser le nom de domaine complet du dispositif vRealize Automation appliance principal ou de tout dispositif vRealize Automation appliance 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.

Désactiver les services inutilisés

Pour préserver les ressources internes lorsqu'une instance externe de vRealize Orchestrator est utilisée, vous pouvez désactiver le service vRealize Orchestrator intégré.

Prérequis

« [Ajouter un autre dispositif vRealize Automation au cluster](#) », page 76

Procédure

- 1 Connectez-vous à la console vRealize Automation appliance.
- 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 appliance, vous devez valider 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 la console vRealize Automation en accédant à `https://vcac-hostname.domain.name/vcac`, où `vcac-hostname.domain.name` est l'adresse de l'équilibrage de charge.
- 3 Après avoir vérifié que le nouveau dispositif vRealize Automation appliance est accessible à l'aide de 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.

Prérequis

- « [Configurer le dispositif vRealize Automation principal](#) », page 70.
- Si votre site inclut plusieurs instances de vRealize Automation appliance, « [Ajouter un autre dispositif vRealize Automation au cluster](#) », page 76.
- Vérifiez que les serveurs d'installation remplissent les conditions requises décrites dans « [Exigences relatives au service Web IaaS et au serveur Model Manager](#) », page 22.
- 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](#) page 79

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](#) page 79

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 appliance.

3 [Choisir un scénario de base de données IaaS](#) page 80

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](#) page 85

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 site Web IaaS supplémentaires](#) page 89

Le composant de site Web permet d'accéder aux fonctionnalités de l'infrastructure dans la console vRealize Automation Web. L'administrateur système peut installer une ou plusieurs instances du composant de site Web.

6 [Installer le service Active Manager Service](#) page 92

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](#) page 94

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](#) page 97

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](#) page 100

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](#) page 101

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.

Suivant

Installez une instance de DEM Orchestrator et au moins une instance de DEM Worker. Reportez-vous à « [Installation des composants Distributed Execution Manager](#) », page 97.

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.

Prérequis

Sur les machines Windows 2012, vous devez désactiver TLS1.2 pour les certificats qui utilisent SHA512. Pour plus d'informations sur la désactivation de TLS1.2, reportez-vous à l'[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.

REMARQUE 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.

Suivant

« [Télécharger le programme d'installation de vRealize Automation IaaS](#) », page 79.

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 appliance.

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

Prérequis

- « [Configurer le dispositif vRealize Automation principal](#) », page 70 et, éventuellement, « [Ajouter un autre dispositif vRealize Automation au cluster](#) », page 76.
- Vérifiez que les serveurs d'installation remplissent les conditions requises décrites dans « [Exigences relatives au service Web IaaS et au serveur Model Manager](#) », page 22.

- 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 À l'aide d'un compte disposant de privilèges d'administrateur, connectez-vous au serveur Windows.
- 3 Pointez un navigateur Web sur l'URL suivante dans le dispositif vRealize Automation appliance.
<https://vrealize-automation-appliance-FQDN:5480/installer>
- 4 Cliquez sur **Programme d'installation d'IaaS**.
- 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 appliance
- 6 Téléchargez le fichier du programme d'installation sur tous les serveurs Windows IaaS sur lesquels vous installez des composants.

Suivant

Installez une base de données IaaS, reportez-vous à « [Choisir un scénario de base de données IaaS](#) », page 80.

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.

REMARQUE 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 obtenir des informations associées sur la configuration de SSL sur le serveur SQL, reportez-vous à l' [article 316898 de la base de connaissances de Microsoft](#).

Tableau 4-13. 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 », page 81.
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 ayant des privilèges dbo pour remplir la base de données, au lieu d'exiger des privilèges sysadmin .	« Préparer une base de données vide », page 82.
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 », page 83.

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.

Prérequis

- Microsoft .NET Framework 4.5.2 ou version ultérieure doit être installé 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 [« Configuration requise du serveur de la base de données IaaS », page 21.](#)
- Téléchargez les scripts du programme d'installation de la base de données IaaS depuis le dispositif vRealize Automation appliance à l'URL suivante.

<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 4-14. 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 appliance 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> .

La base de données a été créée.

Suivant

« [Installer les composants IaaS dans une configuration distribuée](#) », page 77.

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.

Prérequis

- Vérifiez la configuration requise pour l'installation de la base de données. Reportez-vous à « [Configuration requise du serveur de la base de données IaaS](#) », page 21.
- Téléchargez les scripts du programme d'installation de base de données IaaS à partir du dispositif vRealize Automation appliance en accédant à la page <https://vra-va-hostname.domain.name: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 `CreateDatabase.sql` et remplacez toutes les instances des variables de la table avec les valeurs correctes pour votre environnement.

Tableau 4-15. Valeurs de la base de données

Variable	Valeur
<code>\$(DBName)</code>	Nom de la base de données, comme vra. Les noms de base de données ne doivent pas contenir plus de 128 caractères ASCII.
<code>\$(DBDir)</code>	Chemin vers le répertoire de données de la base de données, en excluant la barre oblique finale.
<code>\$(LogDir)</code>	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 `CreateDatabase.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 Cliquez sur **Exécuter**.

Le script s'exécute et crée la base de données.

Suivant

[« Installer les composants IaaS dans une configuration distribuée », page 77.](#)

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 », page 81.](#)

Prérequis

- 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 », page 79.](#)

Procédure

- 1 Cliquez avec le bouton droit sur le fichier d'installation `setup__vra-va-hostname.domain.name@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 appliance 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 de vRealize Automation appliance.
 - 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 appliance. Vous pouvez afficher le certificat vRealize Automation appliance dans le navigateur du client si vous avez accédé à la console 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.
- 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 en savoir plus sur la configuration de SSL sur le serveur SQL, reportez-vous à l'[article 316898 de la base de connaissances de Microsoft](#).
- 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**.

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.

Prérequis

- Installez la base de données IaaS. Pour cela, reportez-vous à la section « [Choisir un scénario de base de données IaaS](#) », page 80.
- Si vous avez installé auparavant d'autres composants dans cet environnement, vérifiez que vous connaissez la phrase secrète qui a été créée. Reportez-vous à « [Phrase secrète de sécurité](#) », page 31.
- 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 site Web IaaS](#) page 86

Un administrateur système installe un composant de site Web pour fournir accès aux capacités de l'infrastructure sur la console Web vRealize Automation.

2 Configurer Model Manager Data page 87

Vous installez le composant Model Manager sur la même machine qui héberge le premier composant du site Web. Vous ne pouvez installer Model Manager Data qu'une seule fois.

Vous pouvez installer des composants supplémentaires du site Web ou installer le service Manager. Reportez-vous à « [Installer des composants de site Web IaaS supplémentaires](#) », page 89 ou « [Installer le service Active Manager Service](#) », page 92.

Installer le premier composant de site Web IaaS

Un administrateur système installe un composant de site Web pour fournir accès aux capacités de l'infrastructure sur la console Web vRealize Automation.

Vous pouvez installer plusieurs composants de site Web, mais un seul peut contenir Model Manager Data. Model Manager Data doit être installé sur le premier composant de site Web que vous créez.

Prérequis

- « [Créer la base de données IaaS à l'aide de l'assistant d'installation](#) », page 83.
- Vérifiez que votre environnement remplit les conditions requises décrites dans « [Exigences relatives au service Web IaaS et au serveur Model Manager](#) », page 22.
- Si vous avez installé auparavant d'autres composants dans cet environnement, vérifiez que vous connaissez la phrase secrète qui a été créée. Reportez-vous à « [Phrase secrète de sécurité](#) », page 31.
- Si vous utilisez des équilibres 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__vra-va-hostname.domain.name@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 appliance 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 de vRealize Automation appliance.
 - 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 appliance. Vous pouvez afficher le certificat vRealize Automation appliance dans le navigateur du client si vous avez accédé à la console 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.
- 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 même machine qui héberge le premier composant du site Web. Vous ne pouvez installer Model Manager Data qu'une seule fois.

Prérequis

« [Installer le premier composant de site Web IaaS](#) », page 86.

Procédure

- 1 Cliquez sur l'onglet **Model Manager Data**.
- 2 Tapez le nom de domaine complet de vRealize Automation appliance dans la zone de texte **Serveur**.
Les adresses IP ne sont pas reconnues.
Par exemple, **vra.mycompany.com**.
- 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 Tapez **administrator@vsphere.local** dans la zone de texte **Nom d'utilisateur** et 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 Tapez le nom de domaine complet du serveur du site Web IaaS dans la zone de texte **serveur IaaS**.

Option	Description
Si vous utilisez un équilibrage de charge	Tapez le nom de domaine complet de l'équilibrage de charge pour le serveur du site Web IaaS. Par exemple, IaaS-load-balancer.eng.mycompany.com . Les adresses IP ne sont pas reconnues.
Sans équilibrage de charge	Tapez le nom de domaine complet du serveur du site Web IaaS. Par exemple, IaaS.eng.mycompany.com . Les adresses IP ne sont pas reconnues.

- 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**.

Suivant

Vous pouvez installer des composants supplémentaires du site Web ou installer le service Manager. Reportez-vous à la section « [Installer des composants de site Web IaaS supplémentaires](#) », page 89 ou « [Installer le service Active Manager Service](#) », page 92.

Installer des composants de site Web IaaS supplémentaires

Le composant de site Web permet d'accéder aux fonctionnalités de l'infrastructure dans la console vRealize Automation Web. L'administrateur système peut installer une ou plusieurs instances du composant de site Web.

N'installez pas Model Manager Data avec le composant de site Web. Seul le premier composant de site Web que vous installez peut contenir Model Manager Data.

Prérequis

- « [Installer un composant de site Web IaaS et Model Manager Data](#) », page 85.
- Vérifiez que votre environnement remplit les conditions requises décrites dans « [Exigences relatives au service Web IaaS et au serveur Model Manager](#) », page 22.
- Si vous avez installé auparavant d'autres composants dans cet environnement, vérifiez que vous connaissez la phrase secrète qui a été créée. Reportez-vous à « [Phrase secrète de sécurité](#) », page 31.
- 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__vra-va-hostname.domain.name@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 appliance 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 de vRealize Automation appliance.
 - 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 appliance. Vous pouvez afficher le certificat vRealize Automation appliance dans le navigateur du client si vous avez accédé à la console 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.
- 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 Entrez les informations du serveur IaaS dans la zone de texte **Serveur IaaS**.

Option	Description
Si vous utilisez un équilibrage de charge	Tapez le nom de domaine complet de l'équilibrage de charge pour le serveur du site Web IaaS. Par exemple, IaaS-load-balancer.eng.mycompany.com .
Sans équilibrage de charge	Tapez le nom de domaine complet du serveur du site Web IaaS. Par exemple, IaaS.eng.mycompany.com .

- 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. Résolez 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**.

Suivant

« [Installer le service Active Manager Service](#) », page 92.

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.

Votre déploiement IaaS nécessite qu'une seule machine Windows exécute de façon active le composant Manager Service. Pour la sauvegarde ou la haute disponibilité, vous devez déployer des machines Windows supplémentaires lorsque vous démarrez manuellement Manager Service si le service actif s'arrête.

IMPORTANT L'exécution simultanée d'un composant Manager Service actif sur plusieurs serveurs Windows IaaS rend vRealize Automation inutilisable.

Prérequis

- Si vous avez installé auparavant d'autres composants dans cet environnement, vérifiez que vous connaissez la phrase secrète qui a été créée. Reportez-vous à « [Phrase secrète de sécurité](#) », page 31.
- (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.
- Microsoft .NET Framework 4.5.2 est installé.
- 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](#) », page 85.

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__vra-va-hostname.domain.name@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 appliance 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 de vRealize Automation appliance.
 - 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 appliance. Vous pouvez afficher le certificat vRealize Automation appliance dans le navigateur du client si vous avez accédé à la console 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.
- 9 Cliquez sur **Suivant**.
- 10 Sélectionnez **Manager Service** sur la page Installation personnalisée du serveur IaaS.
- 11 Entrez les informations du serveur IaaS dans la zone de texte **Serveur IaaS**.

Option	Description
Si vous utilisez un équilibrage de charge	Tapez le nom de domaine complet de l'équilibrage de charge pour le serveur du site Web IaaS. Par exemple, IaaS-load-balancer.eng.mycompany.com .
Sans équilibrage de charge	Tapez le nom de domaine complet du serveur du site Web IaaS. Par exemple, IaaS.eng.mycompany.com .

- 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**.

Suivant

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](#) », page 94.

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](#) », page 100.

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.

Votre déploiement IaaS nécessite qu'une seule machine Windows exécute de façon active le composant Manager Service. Sur les machines qui fournissent le composant de sauvegarde Manager Service, le service doit être arrêté et configuré pour démarrer manuellement.

IMPORTANT L'exécution simultanée d'un composant Manager Service actif sur plusieurs serveurs Windows IaaS rend vRealize Automation inutilisable.

Prérequis

- Si vous avez installé auparavant d'autres composants dans cet environnement, vérifiez que vous connaissez la phrase secrète qui a été créée. Reportez-vous à « [Phrase secrète de sécurité](#) », page 31.
- (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.
- Microsoft .NET Framework 4.5.2 est installé.

- 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](#) », page 85.

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__vra-va-hostname.domain.name@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 appliance 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 de vRealize Automation appliance.
 - 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 appliance. Vous pouvez afficher le certificat vRealize Automation appliance dans le navigateur du client si vous avez accédé à la console 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.
- 10 Cliquez sur **Suivant**.
- 11 Sélectionnez **Manager Service** sur la page Installation personnalisée du serveur IaaS.
- 12 Entrez les informations du serveur IaaS dans la zone de texte **Serveur IaaS**.

Option	Description
Si vous utilisez un équilibrage de charge	Tapez le nom de domaine complet de l'équilibrage de charge pour le serveur du site Web IaaS. Par exemple, IaaS-load-balancer.eng.mycompany.com .
Sans équilibrage de charge	Tapez le nom de domaine complet du serveur du site Web IaaS. Par exemple, IaaS.eng.mycompany.com .

- 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'équilibrage 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**.

Suivant

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](#) », page 100.

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 « [Conditions requises pour Distributed Execution Manager](#) », page 23.

Installer les instances Distributed Execution Manager

Un administrateur système installe au moins une instance DEM travailleur et une instance 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 travailleur sur la même machine.

Prérequis

« [Télécharger le programme d'installation de vRealize Automation IaaS](#) », page 79.

Procédure

- 1 Cliquez avec le bouton droit sur le fichier d'installation `setup__vra-va-hostname.domain.name@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 appliance 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 de vRealize Automation appliance.
 - 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 appliance. Vous pouvez afficher le certificat vRealize Automation appliance dans le navigateur du client si vous avez accédé à la console 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.
- 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'orchestrateur supervise les activités du travailleur, y compris la planification et le traitement préalable des workflows, et contrôle le statut en ligne du DEM travailleur.

- 14 Entrez un nom unique identifiant ce DEM dans la zone de texte **Nom du DEM**.
Si vous prévoyez d'utiliser l'outil de migration, ce nom doit correspondre exactement à celui que vous avez utilisé dans votre installation de vCloud Automation Center 5.2.3. 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
Si vous utilisez un équilibrage de charge	Entrez les noms de domaine complets des équilibres de charge pour les services Manager Service et Model Manager Web Service. Par exemple, manager-load-balancer.eng.mycompany.com:443 et web-load-balancer.eng.mycompany.com:443 .
Sans équilibrage de charge	Entrez les noms de domaine complets des services Manager Service et Model Manager Web Service. Par exemple, manager-service.eng.mycompany.com:443 et model-manager.eng.mycompany.com: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**.

Suivant

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 non standard

Par défaut, le fichier de configuration du travailleur DEM (DynamicOps.DEM.exe.config) pointe vers le chemin d'installation standard de la console System Center Virtual Machine Manager (SCVMM) de Microsoft : {ProgramFiles}\Microsoft System Center 2012\Virtual Machine Manager\bin. L'administrateur système doit modifier le chemin d'installation s'il est installé dans un autre emplacement.

Cette procédure est requise uniquement lorsque vous avez des points de terminaison et des agents SCVMM.

Prérequis

- Si la console SCVMM a été installée dans un autre emplacement, le fichier de configuration du travailleur DEM (situé sous Program Files (x86)\VMware\VCAC\Distributed Execution Manager\<InstanceName>\DynamicOps.DEM.exe.config doit être mis à jour pour modifier le chemin par défaut dans la section assemblyLoadConfiguration afin de pointer vers le nouveau dossier.

```
<assemblyLoadConfiguration>
    <assemblies>
        <!-- List of required assemblies for Scvmm -->
        <add name="Errors" path="{ProgramFiles}\Microsoft System Center 2012\Virtual
            Machine Manager\bin" />
        [...]
    </assemblies>
</assemblyLoadConfiguration>
```

Procédure

- 1 Arrêtez le travailleur DEM.
- 2 Indiquez le chemin d'installation.
- 3 Mettez à jour le fichier `DynamicOps.DEM.exe.config`.
- 4 Redémarrez le travailleur DEM.

Le chemin du travailleur DEM est mis à jour avec le nouveau dossier.

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.

Activez l'accès à la base de données IaaS 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.

Prérequis

- [« Choisir un scénario de base de données IaaS »](#), page 80.
- 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**.

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.

Prérequis

Vérifiez que la base de données SQL Server de vRealize Automation existe. Commencez avec « [Choisir un scénario de base de données IaaS](#) », page 80.

Procédure

- 1 En utilisant un compte disposant de privilèges d'administrateur, connectez-vous au serveur Windows IaaS 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 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.

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](#) », page 104.

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 obtenir plus d'informations sur la stratégie d'exécution PowerShell, reportez-vous à [l'article hh847748 de Microsoft Technet](#). 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 jj149004 de Microsoft Technet](#).

Prérequis

- Connectez-vous en tant qu'administrateur Windows.
- 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 Sélectionnez **Démarrer > Tous les programmes > Version Windows PowerShell > Windows PowerShell**.
- 2 Pour RemoteSigned, exécutez `Set-ExecutionPolicy RemoteSigned`.
- 3 Pour Unrestricted, exécutez `Set-ExecutionPolicy Unrestricted`.
- 4 Vérifiez que la commande n'a pas entraîné d'erreur.

5 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 4-16. 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 », page 103
Provisionner des machines virtuelles via l'intégration avec un environnement Microsoft Hyper-V Server.	« Installation de l'agent Proxy pour Hyper-V ou XenServer », page 109
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 », page 109 ■ « Installation de l'agent EPI pour Citrix », page 116
Provisionner des machines virtuelles via l'intégration avec un environnement XenDesktop.	<ul style="list-style-type: none"> ■ « Installation de l'agent VDI pour XenDesktop », page 113 ■ « Installation de l'agent EPI pour Citrix », page 116
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 », page 119
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 », page 122
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 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 4-17. 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
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
		Supprimer
	Interaction	Configurer les supports CD
		Interaction de console
		Connexion de périphérique
		Mettre hors tension
		Mettre sous tension
		Réinitialiser
		Interrompre
		Installation d'outils

Tableau 4-17. Autorisations requises pour que l'agent vSphere gère une instance de vCenter Server (suite)

Valeur de l'attribut	Autorisation
Configuration	Ajouter un disque existant
	Ajouter un nouveau disque
	Ajouter ou supprimer
	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
	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.

Prérequis

- Les composants IaaS, y compris Manager Service et le site Web, sont installés.
- Vérifiez que vous avez rempli toutes les « [Conditions requises de l'agent vSphere](#) », page 104.
- 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 Automation IaaS](#) », page 79.

Procédure

- 1 Cliquez avec le bouton droit sur le fichier d'installation `setup__vra-va-hostname.domain.name@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 appliance 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 de vRealize Automation appliance.
 - 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 appliance. Vous pouvez afficher le certificat vRealize Automation appliance dans le navigateur du client si vous avez accédé à la console 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.
- 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
Installation d'agent redondant	Installez les agents redondants sur des serveurs distincts. Nommez et configurez les agents redondants de manière identique.
Installation d'agent unique	Sélectionnez un nom unique pour cet agent.

- 13 Configurez une connexion au composant Manager Service.

Option	Description
Si vous utilisez un équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant Manager Service. Par exemple, manager-load-balancer.eng.mycompany.com:443 . Les adresses IP ne sont pas reconnues.
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. Par exemple, manager_service.mycompany.com:443 . Les adresses IP ne sont pas reconnues.

Le port par défaut est 443.

- 14 Configurez une connexion au composant Manager Website.

Option	Description
Si vous utilisez un équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant Manager Website. Par exemple, website-load-balancer.eng.mycompany.com:443 . Les adresses IP ne sont pas reconnues.
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 Website. Par exemple, website_component.mycompany.com:443 . Les adresses IP ne sont pas reconnues.

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.

Suivant

« Configurer l'agent vSphere », page 108.

Configurer l'agent vSphere

Vous pouvez employer l'utilitaire de l'agent proxy pour modifier les configurations initiales qui sont chiffrées dans le fichier de configuration de l'agent `VRMAgent.exe.config` ou pour modifier la stratégie de suppression de machines des plates-formes de virtualisation.

Configurez l'agent vSphere en préparation de la création et de l'utilisation de points de terminaison vSphere à utiliser dans des Blueprints vRealize Automation.

REMARQUE Certaines parties du fichier sont chiffrées, d'autres ne le sont pas. Par exemple, la section `serviceConfiguration` de `VRMAgent.exe.config` n'est pas chiffrée.

Prérequis

Connectez-vous en tant qu'**administrateur système** à la machine sur laquelle vous avez installé l'agent vSphere.

Procédure

- 1 Ouvrez une console de commandes Windows en tant qu'administrateur.
- 2 Accédez au répertoire d'installation des agents.
Par exemple, `cd Program Files (x86)\VMware\VCAC\CD Agents\agent_name.`
- 3 (Facultatif) Entrez `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config get` pour voir les paramètres de configuration actuels.

Voici un exemple de sortie de la commande :

```
managementEndpointName: VCendpoint doDeletes: True
```

- 4 (Facultatif) Entrez la commande `set managementEndpointName` pour modifier le nom du point de terminaison que vous avez configuré lors de l'installation.

Par exemple, `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set managementEndpointName MyEndpoint.`

Vous pouvez modifier cette propriété pour renommer le point de terminaison dans vRealize Automation plutôt que de modifier les points de terminaison.

- 5 (Facultatif) Entrez la commande `set doDeletes` pour configurer la stratégie de suppression de machine virtuelle.

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 <code>VRMDeleted</code> dans vCenter Server.

- 6 (Facultatif) Imposez l'utilisation d'un certificat approuvé pour l'agent vSphere en définissant le paramètre `trustAllCertificates` sur `false` avec l'instruction suivante dans la section `serviceConfiguration` du fichier `VRMAgent.exe.config` :

```
trustAllCertificates = "false"
```

Comme ce paramètre n'est pas chiffré, vous ne pouvez pas utiliser la commande `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set trustAllCertificates false`.

Option	Description
true	(Par défaut) L'agent vSphere ne nécessite pas un certificat approuvé de vCenter Server.
false	L'agent vSphere nécessite un certificat approuvé de vCenter Server.

- 7 Accédez à **Démarrer > Outils d'administration > Services** et redémarrez le service `vRealize Automation Agent – agentname`.

Suivant

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.

REMARQUE Par défaut, Hyper-V n'est pas configuré pour la gestion à distance. Un agent proxy vRealize Automation Hyper-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.

Prérequis

- Les composants IaaS, y compris Manager Service et le site Web, sont installés.
- [« Télécharger le programme d'installation de vRealize Automation IaaS », page 79.](#)

- 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 Automation Hyper-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__vra-va-hostname.domain.name@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 appliance 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 de vRealize Automation appliance.
 - 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 appliance. Vous pouvez afficher le certificat vRealize Automation appliance dans le navigateur du client si vous avez accédé à la console 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.
- 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
Installation d'agent redondant	Installez les agents redondants sur des serveurs distincts. Nommez et configurez les agents redondants de manière identique.
Installation d'agent unique	Sélectionnez un nom unique pour cet 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 au composant Manager Service.

Option	Description
Si vous utilisez un équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant Manager Service. Par exemple, manager-load-balancer.eng.mycompany.com:443 . Les adresses IP ne sont pas reconnues.
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. Par exemple, manager_service.mycompany.com:443 . Les adresses IP ne sont pas reconnues.

Le port par défaut est 443.

- 15 Configurez une connexion au composant Manager Website.

Option	Description
Si vous utilisez un équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant Manager Website. Par exemple, website-load-balancer.eng.mycompany.com:443 . Les adresses IP ne sont pas reconnues.
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 Website. Par exemple, website_component.mycompany.com:443 . Les adresses IP ne sont pas reconnues.

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.

Suivant

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](#) », page 112.

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.

Prérequis

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
```

Suivant

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](#) », page 114 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 »](#), page 102.

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.

Prérequis

- Les composants IaaS, y compris Manager Service et le site Web, sont installés.
- Vérifiez que votre environnement remplit les [« Conditions requises de XenDesktop »](#), page 113.
- [« Télécharger le programme d'installation de vRealize Automation IaaS »](#), page 79.

Procédure

- 1 Cliquez avec le bouton droit sur le fichier d'installation `setup__vra-va-hostname.domain.name@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 appliance 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 de vRealize Automation appliance.
 - 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 appliance. Vous pouvez afficher le certificat vRealize Automation appliance dans le navigateur du client si vous avez accédé à la console 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.
- 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
Installation d'agent redondant	Installez les agents redondants sur des serveurs distincts. Nommez et configurez les agents redondants de manière identique.
Installation d'agent unique	Sélectionnez un nom unique pour cet agent.

- 14 Configurez une connexion au composant Manager Service.

Option	Description
Si vous utilisez un équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant Manager Service. Par exemple, manager-load-balancer.eng.mycompany.com:443 . Les adresses IP ne sont pas reconnues.
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. Par exemple, manager_service.mycompany.com:443 . Les adresses IP ne sont pas reconnues.

Le port par défaut est 443.

- 15 Configurez une connexion au composant Manager Website.

Option	Description
Si vous utilisez un équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant Manager Website. Par exemple, website-load-balancer.eng.mycompany.com:443 . Les adresses IP ne sont pas reconnues.
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 Website. Par exemple, website_component.mycompany.com:443 . Les adresses IP ne sont pas reconnues.

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.

Suivant

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](#) », page 116 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](#) », page 102.

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.

Prérequis

- Les composants IaaS, y compris Manager Service et le site Web, sont installés.
- Vérifiez que vous avez rempli toutes les « [Conditions requises pour Citrix Provisioning Server](#) », page 116
- « [Télécharger le programme d'installation de vRealize Automation IaaS](#) », page 79.

Procédure

- 1 Cliquez avec le bouton droit sur le fichier d'installation `setup__vra-va-hostname.domain.name@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 appliance 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 de vRealize Automation appliance.
 - 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 appliance. Vous pouvez afficher le certificat vRealize Automation appliance dans le navigateur du client si vous avez accédé à la console 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.
- 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
Installation d'agent redondant	Installez les agents redondants sur des serveurs distincts. Nommez et configurez les agents redondants de manière identique.
Installation d'agent unique	Sélectionnez un nom unique pour cet agent.

- 13 Configurez une connexion au composant Manager Service.

Option	Description
Si vous utilisez un équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant Manager Service. Par exemple, manager-load-balancer.eng.mycompany.com:443 . Les adresses IP ne sont pas reconnues.
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. Par exemple, manager_service.mycompany.com:443 . Les adresses IP ne sont pas reconnues.

Le port par défaut est 443.

- 14 Configurez une connexion au composant Manager Website.

Option	Description
Si vous utilisez un équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant Manager Website. Par exemple, website-load-balancer.eng.mycompany.com:443 . Les adresses IP ne sont pas reconnues.
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 Website. Par exemple, website_component.mycompany.com:443 . Les adresses IP ne sont pas reconnues.

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.

Suivant

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.

REMARQUE 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 4-18. 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, reportez-vous à l'adresse http://support.microsoft.com .
Stratégie d'exécution MS PowerShell	La stratégie d'exécution de MS PowerShell doit être définie sur RemoteSigned ou Unrestricted . Pour plus d'informations sur la stratégie d'exécution de PowerShell, exécutez l'une des commandes suivantes à l'invite de commande PowerShell : help about_signing help Set-ExecutionPolicy

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.

Prérequis

- Les composants IaaS, y compris Manager Service et le site Web, sont installés.
- Vérifiez que vous avez rempli toutes les « [Conditions requises pour les scripts Visual Basic](#) », page 119
- « [Télécharger le programme d'installation de vRealize Automation IaaS](#) », page 79.

Procédure

- 1 Cliquez avec le bouton droit sur le fichier d'installation `setup__vra-va-hostname.domain.name@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 appliance 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 de vRealize Automation appliance.
 - 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 appliance. Vous pouvez afficher le certificat vRealize Automation appliance dans le navigateur du client si vous avez accédé à la console 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.
- 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
Installation d'agent redondant	Installez les agents redondants sur des serveurs distincts. Nommez et configurez les agents redondants de manière identique.
Installation d'agent unique	Sélectionnez un nom unique pour cet agent.

- 13 Configurez une connexion au composant Manager Service.

Option	Description
Si vous utilisez un équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant Manager Service. Par exemple, manager-load-balancer.eng.mycompany.com:443 . Les adresses IP ne sont pas reconnues.
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. Par exemple, manager_service.mycompany.com:443 . Les adresses IP ne sont pas reconnues.

Le port par défaut est 443.

- 14 Configurez une connexion au composant Manager Website.

Option	Description
Si vous utilisez un équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant Manager Website. Par exemple, website-load-balancer.eng.mycompany.com:443 . Les adresses IP ne sont pas reconnues.
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 Website. Par exemple, website_component.mycompany.com:443 . Les adresses IP ne sont pas reconnues.

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.

Prérequis

- Les composants IaaS, y compris Manager Service et le site Web, sont installés.
- Vérifiez que vous avez rempli toutes les exigences, en vous reportant à « [Activer les demandes WMI à distance sur les machines Windows](#) », page 122.
- « [Télécharger le programme d'installation de vRealize Automation IaaS](#) », page 79.

Procédure

- 1 Cliquez avec le bouton droit sur le fichier d'installation `setup__vra-va-hostname.domain.name@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 appliance 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 de vRealize Automation appliance.
 - 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 appliance. Vous pouvez afficher le certificat vRealize Automation appliance dans le navigateur du client si vous avez accédé à la console 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.
- 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
Installation d'agent redondant	Installez les agents redondants sur des serveurs distincts. Nommez et configurez les agents redondants de manière identique.
Installation d'agent unique	Sélectionnez un nom unique pour cet agent.

- 13 Configurez une connexion au composant Manager Service.

Option	Description
Si vous utilisez un équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant Manager Service. Par exemple, manager-load-balancer.eng.mycompany.com:443 . Les adresses IP ne sont pas reconnues.
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. Par exemple, manager_service.mycompany.com:443 . Les adresses IP ne sont pas reconnues.

Le port par défaut est 443.

- 14 Configurez une connexion au composant Manager Website.

Option	Description
Si vous utilisez un équilibrage de charge	Entrez le nom de domaine complet et le numéro de port de l'équilibrage de charge pour le composant Manager Website. Par exemple, website-load-balancer.eng.mycompany.com:443 . Les adresses IP ne sont pas reconnues.
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 Website. Par exemple, website_component.mycompany.com:443 . Les adresses IP ne sont pas reconnues.

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.

Tâches post-installation vRealize Automation

5

Après avoir installé vRealize Automation, vous devrez éventuellement effectuer des tâches post-installation.

Ce chapitre aborde les rubriques suivantes :

- [« Remplacement de certificats autosignés par des certificats fournis par une autorité », page 125](#)
- [« Installation de l'agent vRealize Log Insight sur des serveurs IaaS », page 125](#)
- [« Configurer l'accès au locataire par défaut », page 125](#)

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*.

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. Reportez-vous au *Guide d'administration des agents VMware vRealize Log Insight*.

Les dispositifs vRealize Automation appliance incluent l'agent vRealize Log Insight par défaut.

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 la console vRealize Automation en tant qu'administrateur système du locataire par défaut.

- a Accédez à la console vRealize Automation.

Option	Description
Sans équilibrage de charge	https://vrealize-appliance-hostname.domain.name/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 dans l'onglet **Administrateurs**.
- 7 Attribuez à vos utilisateurs locaux les rôles d'administrateur de locataires et d'administrateur IaaS.
 - 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 IaaS** et appuyez sur Entrée.
L'administrateur IaaS 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**.

Suivant

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 IaaS 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. Pour obtenir un exemple de demande d'élément et d'exécution d'action manuelle d'utilisateur, reportez-vous au document *Installation et configuration de vRealize Automation pour le scénario Rainpole*.

Dépannage de l'installation de vRealize Automation

6

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 aborde les rubriques suivantes :

- « [Emplacement des journaux par défaut](#) », page 127
- « [Restauration d'une installation qui a échoué](#) », page 128
- « [Création d'un bundle de support vRealize Automation](#) », page 130
- « [Dépannage de l'installation générale](#) », page 131
- « [Dépannage du dispositif vRealize Automation](#) », page 134
- « [Dépannage des composants IaaS](#) », page 137
- « [Dépannage des erreurs de connexion](#) », page 144

Emplacement des journaux par défaut

Consultez les fichiers journaux système et des produits pour obtenir des informations sur une installation ayant échoué.

Les chemins d'accès aux fichiers présentés sont les chemins par défaut. Si vous avez installé IaaS dans un autre répertoire, accédez plutôt à votre répertoire d'installation personnalisé.

REMARQUE 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 plus d'informations, visitez [VMware Solution Exchange](#).

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

REMARQUE 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

REMARQUE 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.

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 Server
- WAPI de vRealize Automation

REMARQUE 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.

REMARQUE 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, le vCAC et le WAPI ont été supprimés et que les pools d'applications RepositoryAppPool, vCACAppPool et WapiAppPool ont été également supprimés.

Tableau 6-1. 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 le DEM Worker.
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 appliance. 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 Dans un navigateur Web, ouvrez l'interface de gestion du dispositif vRealize Automation appliance.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Connectez-vous en tant que root et cliquez sur **Paramètres vRA > Cluster**.
- 3 Cliquez sur **Créer un bundle de support**.
- 4 Cliquez sur **Télécharger** et enregistrez le fichier du bundle de support sur votre système.

Les bundles de support incluent des informations sur le dispositif vRealize Automation appliance et les serveurs Windows IaaS. Si vous perdez la connectivité entre le dispositif vRealize Automation appliance et les composants IaaS, il manque peut-être au bundle de support les 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.

Pour obtenir une procédure de sauvegarde permettant de collecter les bundles de journaux de composant IaaS, reportez-vous à l'[article 2078179 de la base de connaissances VMware](#).

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. Par exemple, en fonction de l'équilibrage de charge que vous utilisez, modifiez le paramètre de délai d'expiration de l'équilibrage de charge dans votre fichier de configuration `Web ssl.conf`, `httpd.conf` ou autre.
- 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 appliance.

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

Pour chaque serveur vRealize Automation appliance et tous les serveurs Windows sur lesquels des composants IaaS seront installés, activez la synchronisation de l'heure décrite dans les rubriques suivantes :

- « [Activer la synchronisation de l'heure sur le dispositif vRealize Automation](#) », page 54
- « [Activer la synchronisation de l'heure sur le serveur Windows](#) », page 57

Pour consulter une présentation du chronométrage de vRealize Automation, reportez-vous à la section « [Synchronisation de l'heure](#) », page 32.

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.

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

Prérequis

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**).

Procédure

- 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 le fichier vcac-config.exe.config et localisez l'adresse de référentiel : <add key="repositoryAddress" value="https://[IaaS address]:443/repository/" />
- 2 Recherchez cette adresse dans Internet Explorer.
- 3 Parcourez tous les messages d'erreur éventuels concernant des problèmes de confiance de certificat.
- 4 Obtenez un rapport de sécurité dans Internet Explorer et utilisez-le pour déterminer pourquoi ce certificat n'est pas approuvé.

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.

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

Prérequis

Obtenez de votre administrateur des noms, des numéros de port et des informations d'identification de serveurs proxy.

Procédure

- 1 Dans un navigateur Web, accédez à la console de gestion de vRealize Automation appliance :
`https://appliance-FQDN-or-IP-address:5480`
- 2 Connectez-vous avec le nom d'utilisateur **root** et le mot de passe que vous avez défini lors du déploiement du dispositif.
- 3 Cliquez sur l'onglet **Réseau**.
- 4 Entrez le nom de domaine complet ou l'adresse IP, et le numéro de port du serveur proxy de votre site.
- 5 Si votre serveur proxy nécessite des informations d'identification, entrez le nom d'utilisateur et le mot de passe.
- 6 Cliquez sur **Enregistrer les paramètres**.

Suivant

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 les utilisateurs de VMware Identity Manager de se connecter](#) », page 145.

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.

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

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.

Procédure

- 1 Connectez-vous à la console vRealize Automation appliance en tant que 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.p
y --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.p
y --host $CURRENT_VA_HOSTNAME --username $SSO_ADMIN_USERNAME --password
$SSO_ADMIN_PASSWORD --workflowid ef00fce2-80ef-4b48-96b5-fdee36981770 --
configurationAdminPassword $CONFIGURATIONADMIN_PASSWORD
```

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

Les programmes d'installation échouent à se télécharger depuis le dispositif vRealize Automation appliance.

Problème

Les programmes d'installation ne se téléchargent pas lors de l'exécution de `setup__vra-va-hostname.domain.name.exe`.

Cause

- Problèmes de connectivité réseau lors de la connexion à la machine vRealize Automation appliance.
- Impossible de se connecter à la machine vRealize Automation appliance, car la machine est inaccessible ou ne répond pas avant l'expiration du délai de connexion.

Solution

- 1 Vérifiez que vous pouvez vous connecter au dispositif vRealize Automation appliance en tapant l'URL suivante sur un navigateur Web.
`https://vra-va-hostname.domain.name`
- 2 Consultez les autres rubriques de dépannage de vRealize Automation appliance.
- 3 Téléchargez le fichier de configuration et reconnectez-vous au dispositif vRealize Automation appliance.

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.

Problème

Vous vous connectez à vRealize Automation appliance 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**Prérequis**

Connectez-vous au dispositif virtuel qui affiche l'erreur.

REMARQUE Si vos dispositifs virtuels sont exécutés sous un équilibrage de charge, vous devez vérifier chacun d'entre eux.

Procédure

- 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.

Suivant

Connectez-vous à la page Locataire pour vérifier que vous pouvez vous connecter sans erreur.

Échec du démarrage d'Identity Manager 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 :

Erreur de création du bean portant le nom « liquibase » défini dans la ressource de chemin de classe [spring/datastore-wireup.xml] : Échec de l'invocation de la méthode d'initialisation ; exception liquibase imbriquée. Exception de verrouillage : acquisition le verrouillage du journal contre les modifications. Actuellement verrouillé par fe80:0:0:0:250:56ff:fea8:7d0c%eth0 (fe80:0:0:0:250:56ff:fea8:7d0c%eth0) depuis le 29/10/15

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 au dispositif vRealize Automation appliance en tant que racine via SSH.
- 2 Exécutez la commande `service horizon-workspace` pour arrêter le service horizon-workspace.
- 3 Exécutez la commande `su postgres` pour devenir un utilisateur postgres.
- 4 Exécutez la commande `psql vcac`.
- 5 Exécutez la requête SQL suivante : `"update "databasechangelock" set locked=FALSE, lockgranted=NULL, lockedby=NULL where id=1;"`
- 6 Exécutez la commande SQL `select * depuis databasechangelock`.
La sortie devrait afficher une valeur de « f » pour verrouillé.
- 7 Démarrez le service horizon-workspace au moyen de la commande `service horizon-workspace start`.

Attributions de rôles de dispositifs incorrectes après basculement

Après un basculement, les nœuds master et de réplica vRealize Automation appliance 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 appliance, vous arrêtez le nœud master de la base de données ou le rendez inaccessible. Vous utilisez la console 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 Base de données dans sa console de gestion indique toujours que le nœud est le nœud master même s'il ne l'est plus. Les tentatives d'utilisation d'une console 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 vRealize Automation appliance.
- Pour que vRealize Automation remplace un ancien nœud master dans le cluster, laissez l'ancienne machine venir en ligne. Ouvrez ensuite la console de gestion du nouveau nœud master. Recherchez l'ancien nœud signalé comme `invalid` dans l'onglet Base de données, puis cliquez sur son bouton **Réinitialiser**.

Après la réinitialisation, vous pouvez restaurer l'ancien nœud dans le pool d'équilibrage de charge des nœuds vRealize Automation appliance.

- 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 vRealize Automation appliance.

- Tant que vous n'avez pas réinitialisé ou remis correctement dans le cluster un ancien nœud master, n'utilisez pas sa console de gestion pour les opérations de gestion de clusters, même si le nœud est revenu en ligne.
- Après la réinitialisation ou la nouvelle jonction, vous pouvez promouvoir de nouveau l'ancien nœud au rang de nœud master.

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.

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 appliance et les certificats du dispositif SSO.

Problème

Des erreurs d'autorisation s'affichent lorsque vous utilisez des fonctionnalités IaaS.

Cause

Les 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.

REMARQUE 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 du dispositif vRealize Automation appliance 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 EM et du serveur de site Web du dispositif vRealize Automation appliance a échoué en raison de paramètres `msiexec` 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 appliance 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 au dispositif vRealize Automation appliance en tapant l'URL suivante dans un navigateur Web : <https://vra-va-hostname.domain.name>.

■ 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, accédez à `https://<ip-web>/repository/data/MetaModel.svc` et vérifiez qu'aucune erreur de certificat ne s'affiche dans votre navigateur.

■ Incompatibilité du 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 root 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, vérifiez l'état du service MetaModel à l'adresse `https://<ip-web>/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 [l'article 2564571 de la base de connaissances](#).

Solution

- 1 Redémarrez votre machine ou explorez.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 Coordinateur) 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**.

REMARQUE 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 vRealize Automation appliance.
`https://virtualappliancename/vcac/tenantname`
 - 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 nœuds IaaS qui sont clonés à partir d'un modèle sur lequel MS DTC est installé, contiennent des identifiants dupliqués pour MS DTC, empêchant la communication entre les nœuds.

Problème

Le service de gestion IaaS échoue et affiche l'erreur suivante dans le journal de service 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 nœud IaaS sur lequel MS DTC est installé, les deux clones utilisent le même identifiant unique pour MS DTC. Échec de la communication entre les nœuds.

Solution

- 1 Ouvrez une invite de commande d'administrateur.
- 2 Exécutez la commande suivante : `msdtc -uninstall`
- 3 Redémarrez la machine virtuelle.
- 4 Ouvrez une invite de commande séparée et exécutez la commande suivante :
`msdtc -install <manager-service-host>.`

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 appliance, les dispositifs doivent pouvoir s'identifier entre eux par un nom d'hôte court. Sinon, vous ne pouvez pas vous connecter.

Problème

Vous configurez vRealize Automation pour la haute disponibilité en installant un dispositif vRealize Automation appliance 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 vRealize Automation appliance ne forment pas correctement un cluster haute disponibilité tant qu'ils ne peuvent pas résoudre les noms d'hôte courts des hôtes du cluster.

Solution

Pour permettre à un cluster de dispositifs vRealize Automation appliance haute disponibilité de résoudre des noms d'hôtes courts, adoptez l'une des approches suivantes. Vous devez modifier tous les dispositifs du cluster.

Procédure

- Modifiez ou créez une ligne de recherche dans `/etc/resolv.conf`. La ligne doit contenir les domaines qui reçoivent des dispositifs vRealize Automation appliance. Séparez plusieurs domaines avec des espaces. Par exemple :

`search eng.mycompany.com tech.mycompany.com`
- Modifiez ou créez des lignes de domaine dans `/etc/resolv.conf`. Chaque ligne doit contenir un domaine qui reçoit des dispositifs vRealize Automation appliance. Par exemple :

`domain eng.mycompany.com`
- Ajoutez des lignes au fichier `/etc/hosts` de telle sorte que chaque nom court de dispositif vRealize Automation appliance soit mappé à son nom de domaine complet. Par exemple :

<code>node1</code>	<code>node1.eng.mycompany.com</code>
<code>node2</code>	<code>node2.eng.mycompany.com</code>

Le proxy empêche les utilisateurs de VMware Identity Manager de se connecter

La configuration d'un proxy peut empêcher les utilisateurs de VMware Identity Manager de se connecter.

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**Prérequis**

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](#) », page 133.

Procédure

- 1 Connectez-vous à la console de vRealize Automation appliance en tant que 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=vra-hostname`

Par exemple : `NO_PROXY="localhost, 127.0.0.1, vra.system.mycompany.com"`
- 4 Enregistrez et fermez le proxy.
- 5 Redémarrez le service Horizon Workspace en saisissant la commande suivante.

`service horizon-workspace restart`

Installation silencieuse de vRealize Automation

7

vRealize Automation inclut une option permettant une installation silencieuse par script.

L'installation silencieuse utilise un exécutable qui fait référence à un fichier de réponses basé sur texte dans lequel vous pouvez préconfigurer les noms de domaine complets du système, les informations d'identification du compte et d'autres paramètres qui sont généralement ajoutés lors d'une installation conventionnelle manuelle ou basée sur assistant. 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

Ce chapitre aborde les rubriques suivantes :

- [« Effectuer une installation silencieuse de vRealize Automation », page 147](#)
- [« Effectuer une installation silencieuse de l'agent de gestion de vRealize Automation », page 148](#)
- [« Fichier de réponses pour installation silencieuse de vRealize Automation », page 149](#)
- [« La ligne de commande d'installation de vRealize Automation », page 150](#)

Effectuer une installation silencieuse de vRealize Automation

Vous pouvez effectuer une installation silencieuse sans assistance de vRealize Automation à partir d'un vRealize Automation appliance nouvellement déployé.

Prérequis

- Déployez un vRealize Automation appliance, mais sans vous connecter ni démarrer l'assistant d'installation.
- 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 », page 148](#).

Procédure

- 1 Connectez-vous à la console vRealize Automation appliance en tant que 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.

Prérequis

- Déployez le vRealize Automation appliance.
- Créez ou identifiez vos serveurs Windows IaaS et configurez leurs conditions préalables.

Procédure

- 1 Sur le serveur Windows IaaS, pointez un navigateur Web vers l'URL suivante sur le vRealize Automation appliance :

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

- 2 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.

- 3 Ouvrez `InstallManagementAgent.ps1` dans un éditeur de texte.

- 4 Vers le haut du fichier de script, ajoutez les paramètres spécifiques à votre déploiement.

- L'URL du vRealize Automation appliance
`https://vrealize-automation-appliance-FQDN:5480`
- Informations d'identification du compte d'utilisateur racine de vRealize Automation appliance
- 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
- 5 Enregistrez et fermez le fichier `InstallManagementAgent.ps1`.
 - 6 Pour installer silencieusement l'agent de gestion, double-cliquez sur `InstallManagementAgent.ps1`.
 - 7 (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 vRealize Automation appliance 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 vRealize Automation appliance
- Informations d'identification du compte d'utilisateur racine de vRealize Automation appliance
- 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.

Informations de base sur la ligne de commande d'installation de vRealize Automation

L'interface de ligne de commande d'installation de vRealize Automation permet trois opérations de base.

Les opérations de base affichent les ID de nœud de vRealize Automation, exécutent des commandes ou affichent les informations d'aide. Pour présenter ces opérations sur l'affichage de la console, entrez la commande suivante sans option ni qualificateur.

```
vra-command
```

Afficher les ID de nœud

Vous devez connaître les ID de nœud vRealize Automation pour exécuter les commandes sur les systèmes cibles appropriés. Pour afficher les ID de nœud, entrez la commande suivante.

```
vra-command list-nodes
```

Notez les ID de nœud avant d'exécuter les commandes.

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 choisies par l'utilisateur.

Afficher l'aide

Pour afficher les informations d'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 appliance à une installation existante
- Définition du nom de l'hôte auquel 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 vRealize Automation appliance, 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
```


Index

A

- accès à la base de données laaS, activation par l'utilisateur du service **100**
- Administrateurs laaS, création **125**
- Agent de gestion
 - désinstaller **37, 44**
 - installation **36, 43**
 - installation silencieuse **148**
 - installer **37, 44**
- agent EPI, installation pour les scripts Visual Basic **119, 120**
- agent proxy, échec de la désinstallation **141**
- agent VDI pour XenDesktop, installation **113**
- agent vSphere
 - autorisations requises **104**
 - configuration prise en charge pour la simultanéité **104**
- agents
 - activer les demandes WMI à distance **122**
 - agents d'intégration **17**
 - agents WMI **17**
 - choisir le scénario d'installation **103**
 - conditions requises pour l'écriture de scripts Visual Basic **119**
 - configuration d'agents vSphere **108**
 - configuration de Hyper-V **112**
 - configuration de XenServer **112**
 - emplacement et conditions d'installation **103**
 - EPI PowerShell **17**
 - Hyper-V **109**
 - installation **102**
 - installation d'agents Citrix **117**
 - installation d'agents vSphere **105**
 - installation de l'agent EPI pour Citrix **116**
 - installation de l'agent EPI pour l'écriture de scripts VB **119**
 - installation de WMI **122**
 - installation de XenDesktop **114**
 - installation pour les scripts Visual Basic **120**
 - VDI PowerShell **17**
 - XenServer **109**
- agents Citrix, installation **117**
- agents Hyper-V, installation **109**
- agents proxy, installation et configuration pour vSphere **103**
- agents proxy de virtualisation **17**

- agents proxy vSphere, installation et configuration **103**
- agents vSphere
 - configuration **108**
 - exiger un certificat approuvé **108**
 - installation **105**
- agents WMI
 - activer les demandes WMI **122**
 - installation **122**
- agents XenServer, installation **109**
- assistant d'installation, déploiement d'entreprise **42**
- Assistant d'installation, présentation **33**
- authentification **101**
- authentification au moment de l'exécution **101**
- Authentification laaS, panne **139**
- authentification SQL **101**
- authentification Windows **101**

B

- base de données
 - configuration requise **21**
 - création à l'aide de l'assistant **83**
 - préparation de la base de données laaS **80**
- base de données laaS
 - configuration du service Windows pour accès **100**
 - configuration pour base de données SSL sécurisée **60, 80–83**
 - création de la base de données **82**
 - création de la base de données à l'aide de l'assistant **83**
 - création de la base de données manuellement **81**
 - spécification de la base de données SQL **60**
- bundle de support, création **130**

C

- cas d'utilisation, installation silencieuse **147**
- certificats
 - basculer depuis les certificats autosignés **125**
 - relations de confiance **65**
- certificats enchaînés, ordre **30**
- certificats SSL, extraction **31**
- chaînes de certificats, ordre **30**

- chemin de déploiement
 - choisir **11**
 - installation distribuée **11**
- Citrix, installation de l'agent EPI **116**
- Clés privées RSA, commande d'extraction **31**
- clusters vRealize Appliance;association **76**
- clusters;association **76**
- composant du site Web, installation **85–87, 89**
- composants d'installation
 - choisir un chemin de déploiement **11**
 - dispositif VMware vRealize Automation **15**
 - laas (Infrastructure as a Service) VMware **15**
 - SSO **14**
 - Vérification des conditions préalables **60**
- Composants de l'infrastructure, installation **58**
- composants laaS
 - dépannage **137**
 - inscription **62**
 - installation **57**
 - installation dans une configuration distribuée **77**
- Composants laaS, définitions **64**
- conditions d'installation
 - conditions requises pour laaS **22**
 - configuration requise du port **26**
 - environnements de déploiement **20**
 - informations d'identification **29**
 - machine virtuelle **20**
 - matériel **20**
 - sécurité **30**
 - Serveur Windows **21**
 - système d'exploitation **20**
 - utilisateurs **29**
 - XenDesktop **113**
- conditions préalables
 - considérations concernant le navigateur **20**
 - vérification **60**
- conditions requises, DEM **23**
- conditions requises Java, pour la base de données MSSQL **22**
- conditions requises pour le serveur, serveur laaS ou Windows **22**
- Configuration de contenu initial, créer le mot de passe **42, 49**
- configuration requise
 - base de données **21**
 - SQL **21**
- configurer, dispositif vRealize Automation **71**
- contrôles de santé **65**
- création de contenu initial, dépannage **133**

D

- dem
 - conditions requises de SCVMM **25**

- configuration requise de Red Hat **25**
- Configuration requise pour Amazon Web Services EC2 **24**

DEM

- à propos de l'installation **97**
- conditions requises **23**
- configuration requise pour Ooerstack **25**
- configuration requise pour PowerVC **25**
- échec de l'installation **138**
- installation **97**
- dépannage
 - apparition de pages blanches **132**
 - demandes de machines **142**
 - emplacements des journaux **127**
 - heures du serveur désynchronisées **131**
 - nœud master incorrect **136**
 - nœuds laaS clonés **143**
 - programme d'installation d'laaS **138**
- dépannage de l'installation **131**
- dépannage, installation **127**
- dépassement du délai de l'équilibrage de charge
 - avant achèvement, modification du paramètres de délai d'expiration de l'équilibrage de charge **131**
- déploiement d'entreprise, installer avec assistant **43**
- déploiement distribué
 - désactiver les services inutilisés **77**
 - installer avec assistant **43**
 - présentation de l'installation **13**
 - validation **77**
- déploiement minimal, présentation de l'installation **12**
- Déploiements minimaux, installer avec l'assistant d'installation **35**
- désinstaller, installation ayant échoué **129**
- Désinstaller, installation ayant échoué **129**
- dispositif vRealize Automation, déploiement **68**
- dispositif vRealize Realize Automation **52**
- dispositifs, configuration d'instances supplémentaires **75**
- dispositifs vRealize Automation, dépannage **134**
- Distributed Execution Manager, , voir DEM
- Distributed Transaction Coordinator (DTC) **21**
- DTC (Distributed Transaction Coordinator) **21**

E

- échec d'installation, serveurs désynchronisés **131**
- échec de connexion
 - dépannage **144**
 - serveurs désynchronisés **131**
- échec de la demande de la machine **142**
- Empreinte digitale SSL d'agent de gestion, emplacement **36, 43**

- équilibrages de charge
 - configuration **70**
 - contrôles de santé **65**
- erreur interne, ajout d'un point de terminaison XaaS **141**
- erreurs de connexion, dépannage **144**
- exigences **116**

F

- Federal Information Processing Standard (FIPS) **140**
- fichier de réponses, installation silencieuse **149**
- fichier Encryption.key, définition d'autorisations **135**
- fichiers PEM, commande d'extraction **31**
- fichiers pfx, configurer une approbation de certificat **66**
- FIPS (Federal Information Processing Standard) **140**

H

- Hyper-V
 - agent **109**
 - agent proxy **109**
 - conditions requises **109**
- hyperviseur, conditions requises **109**

I

- IaaS
 - agents **17**
 - télécharger le programme d'installation **79**
- IaaS Manager Service, configuration requise **23**
- IaaS VMware, Model Manager **15**
- IaaS VMware, site Web IaaS **15**
- ID de nœud **150**
- identity manager, échec du démarrage **135**
- incompatibilité de nom de certificat **139**
- informations mises à jour **9**
- installation
 - configuration de dispositifs VMware vCloud Automation Center **70**
 - considérations concernant le navigateur **20**
 - dépannage **127**
 - dispositif vRealize Automation **52, 70**
 - DNS et résolution du nom d'hôte **19**
 - exécution **62**
 - feuille d'activité **66**
 - fin **40, 48**
 - post-installation **125**
 - préparation **19**
 - présentation **11**
 - présentation de l'installation minimale **52**
 - présentation du déploiement distribué **13**
 - présentation du déploiement minimal **12**

- spécification d'agents **61**
- spécification de gestionnaires **61**
- télécharger le programme d'installation d'IaaS **79**

- Installation, utilisation de la console de gestion **51**
- installation ayant échoué, journaux **127**
- installation distribuée
 - désinstallation **129**
 - présentation **63**
- Installation distribuée IaaS **64**
- installation minimale, désinstallation **129**
- installation silencieuse
 - Agent de gestion **148**
 - cas d'utilisation **147**
 - fichier de réponses **149**
 - vRealize Automation **147**
- Instances Distributed Execution Manager, Voir aussi DEM

J

- journaux
 - collecter **130**
 - emplacements **127**
- Journaux
 - dépannage **127**
 - IaaS **127**

L

- la connexion en tant qu'administrateur IaaS échoue **144**
- ligne de commande **150, 151**
- locataires, configuration du locataire par défaut **125**
- Log Insight **125**

M

- magasin d'identités, conditions requises du domaine **29**
- Manager Service
 - configuration requise **23**
 - définition **64**
 - installation **92, 94**
- Manager Service, approbation de certificat **66**
- Message d'erreur système **135**
- Model Manager
 - définition **64**
 - location multiple sécurisée **15**
 - logique métier modifiable **15**
 - modèle de données unifié **15**
 - résolution de problèmes d'échec d'installation **139**
 - stratégies d'exécution **15**
- Model Manager data, installation **85–87, 89**
- Model Manager Web **15**

mot de passe, limitations **21**

N

nœud master incorrect **136**

Nœuds IaaS clonés **143**

nom d'hôte XenServer, paramètre **114**

O

Openstack, configuration requise pour DEM **25**

Outil de vérification des conditions préalables,
exécuter l'assistant d'installation **39, 46**

P

paramètre d'installation, validation **41, 48**

paramètres d'heure des dispositifs virtuels, avec
l'assistant Installation **39, 46**

paramètres de compte, spécification **60**

paramètres de déploiement, spécification **40, 47**

paramètres de serveur, spécification **60**

Personnalisations des e-mails **143**

Points de terminaison

configuration requise pour Ooenstack
DEM **25**

Configuration requise pour PowerVC DEM **25**

post-installation **125**

PowerShell, définition sur RemoteSigned **102**

PowerVC, configuration requise pour DEM **25**

préparation de l'installation, synchronisation de
l'heure **32**

problèmes de certificat approuvé **139**

programme d'installation d'IaaS
dépannage **138**

téléchargement **59**

proxy **145**

S

scénario de déploiement

déploiement distribué **63**

déploiement minimal **51**

installation minimale **11**

scénarios, choisir l'installation de l'agent **103**

scripts Visual Basic

installation de l'agent EPI **119**

installation des agents EPI **120**

sécurité

certificats **30**

certificats IaaS **58, 79**

logiciels tiers **32**

phrase secrète **31**

relations de confiance **65**

serveur de provisionnement **116**

services IaaS, vérification **101**

snapshots, création **40, 47**

SQL, configuration requise **21**

synchronisation de l'heure

activation sur une machine Windows **57**

serveurs **54, 75**

T

tâches post-installation, configuration du service
Windows pour accéder à la base de
données IaaS **100**

téléchargement d'installation, dépannage **134**

travailleur DEM, connexion à SCVMM **99**

type d'installation

connexion **59**

sélection **59**

V

validation du certificat **137**

vCloud Suite, attribution de licence **7**

Visual Basic, conditions requises pour l'écriture
de scripts **119**

VMware IaaS

distributed execution manager **16**

service de gestion **16**

Vmware IaaS, base de données **16**

VMware Identity Manager **145**

vRealize Appliance

configuration **55**

déploiement **33, 52**

vRealize Orchestrator, utiliser des mises en
œuvre externes pour les déploiements
de haute disponibilité **63**

W

WAPI, échec de l'installation **138**

X

XenDesktop

conditions d'installation **113**

Installation de l'agent **114**

installation de l'agent VDI **113**

XenServer

agent **109**

agent proxy **109**