

Installation et mise à niveau de vRealize Automation

21 juillet 2021

vRealize Automation 7.5

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

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

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

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

Copyright © 2017-2021 VMware, Inc. Tous droits réservés. [Informations relatives aux copyrights et marques commerciales.](#)

Table des matières

1	Installation ou mise à niveau de vRealize Automation	4
	Configuration sécurisée de vRealize Automation	4
	vRealize Automation Présentation de la sécurisation de la ligne de base	4
	Vérification de l'intégrité du support d'installation	5
	Sécurisation renforcée de l'infrastructure logicielle du système VMware	6
	Vérification des logiciels installés	7
	Correctifs et avis de sécurité de VMware	8
	Configuration sécurisée	8
	Configuration de la sécurité réseau des hôtes	45
	Audit et journalisation	61
	Architecture de référence de vRealize Automation	62
	Recommandations relatives au déploiement initial et à la configuration	62
	Déploiement de vRealize Automation	63
	Éléments à prendre en compte pour le déploiement de vRealize Business for Cloud	66
	Évolutivité de vRealize Automation	66
	Évolutivité de vRealize Business for Cloud	69
	Éléments à prendre en compte pour la configuration de la haute disponibilité vRealize Automation	70
	Éléments à prendre en compte pour la haute disponibilité de vRealize Business for Cloud	72
	Spécifications matérielles et capacité maximale de vRealize Automation	72
	Configuration requise pour un petit déploiement de vRealize Automation	75
	Configuration requise d'un déploiement moyen de vRealize Automation	80
	Configuration requise pour un grand déploiement de vRealize Automation	86
	Déploiements de données de centre de données multiples dans vRealize Automation	92
	Installation de vRealize Automation	93
	Présentation de l'installation	93
	Préparation à l'installation	102
	Déploiement du dispositif vRealize Automation	121
	Installation avec l'assistant d'installation	126
	Les interfaces d'installation standard	155
	Installation silencieuse	242
	Tâches post-installation	249
	Dépannage d'une installation	267
	Mise à niveau et migration de vRealize Automation	298
	Mise à niveau de vRealize Automation 7.1 ou version ultérieure vers la version 7.5	301
	Mise à niveau de vRealize Automation 6.2.5 vers la version 7.5	366
	Migration de vRealize Automation	441

Installation ou mise à niveau de vRealize Automation

1

Vous pouvez installer vRealize Automation pour la première fois ou vous pouvez mettre à niveau votre environnement actuel vers la version la plus récente.

Ce chapitre contient les rubriques suivantes :

- [Configuration sécurisée de vRealize Automation](#)
- [Architecture de référence de vRealize Automation](#)
- [Installation de vRealize Automation](#)
- [Mise à niveau et migration de vRealize Automation](#)

Configuration sécurisée de vRealize Automation

La configuration sécurisée permet de vérifier, de configurer et de mettre à jour le profil de sécurité d'un déploiement de vRealize Automation conformément aux directives de VMware.

La configuration sécurisée couvre les points suivants :

- Sécurité de l'infrastructure logicielle
- Sécurité de la configuration déployée
- Sécurité du réseau hôte

vRealize Automation Présentation de la sécurisation de la ligne de base

VMware fournit des recommandations complètes pour vous aider à vérifier et à configurer une ligne de base sécurisée pour votre système vRealize Automation.

Utilisez les outils et les procédures spécifiés par VMware pour vérifier et maintenir une configuration de ligne de base avec sécurisation renforcée sur votre système vRealize Automation. Certains composants vRealize Automation sont installés dans un état sécurisé ou partiellement sécurisé, mais vous devez vérifier la configuration de chaque composant en fonction des recommandations de sécurité de VMware, des stratégies de sécurité de l'entreprise et des menaces connues.

Approche de la sécurité de vRealize Automation

L'approche de la sécurité de vRealize Automation suppose un environnement sécurisé de façon holistique, reposant sur la configuration du système et du réseau, les stratégies de sécurité de l'organisation et les meilleures pratiques de sécurité.

Lors de la vérification et de la configuration de la sécurisation renforcée d'un système vRealize Automation, tenez compte de chacun des éléments suivants, tels que définis par les recommandations de sécurisation renforcée de VMware.

- Déploiement sécurisé
- Configuration sécurisée
- Sécurité du réseau

Afin de garantir la sécurisation renforcée de votre système, suivez les recommandations de VMware et vos stratégies locales de sécurité, car elles se rapportent à chacun de ces concepts.

Composants système

Lors de la préparation de la sécurisation renforcée et de la configuration sécurisée de votre système vRealize Automation, assurez-vous de comprendre l'ensemble des composants et leurs interactions au niveau du système.

Tenez compte des composants suivants lors de la planification et de l'implémentation d'un système sécurisé.

- dispositif vRealize Automation
- Composant IaaS

Pour vous familiariser avec vRealize Automation et comprendre l'interaction entre les composants, reportez-vous à la section [Fondements et concepts](#) du centre de documentation de VMware vRealize Automation. Pour plus d'informations sur les déploiements et l'architecture types de vRealize Automation, reportez-vous à la section [Architecture de référence de vRealize Automation](#).

Vérification de l'intégrité du support d'installation

Les utilisateurs doivent toujours vérifier l'intégrité du support d'installation avant d'installer un produit VMware.

Vérifiez toujours le hachage SHA1 après avoir téléchargé un fichier ISO, un bundle hors ligne ou un correctif, afin de garantir l'intégrité et l'authenticité des fichiers téléchargés. Si vous obtenez des supports physiques de VMware et si le sceau de sécurité a été rompu, renvoyez le logiciel à VMware en demandant son remplacement.

Après avoir téléchargé le support, utilisez la somme MD5/SHA1 pour vérifier l'intégrité du téléchargement. Comparez la sortie de hachage MD5/SHA1 avec la valeur publiée sur le site Web de VMware. Les hachages SHA1 ou MD5 doivent correspondre.

Pour plus d'informations sur la vérification de l'intégrité du support d'installation, reportez-vous à l'article <http://kb.vmware.com/kb/1537>.

Sécurisation renforcée de l'infrastructure logicielle du système VMware

Dans le cadre du processus de sécurisation renforcée, évaluez l'infrastructure logicielle déployée qui prend en charge votre système VMware et vérifiez qu'elle respecte les directives de sécurisation renforcée de VMware.

Avant de renforcer la sécurité de votre système VMware, identifiez et corrigez les défauts de sécurité de l'infrastructure logicielle utilisée, afin de créer un environnement totalement renforcé et sécurisé. Vous devez notamment prendre en compte les composants du système d'exploitation, les logiciels de prise en charge et de base de données. Traitez les problèmes de sécurité à ce niveau, et sur les autres composants impliqués, selon les recommandations du fabricant et autres protocoles de sécurité applicables.

Sécurisation renforcée de l'environnement VMware vSphere ®

Évaluez l'environnement de VMware vSphere ® et assurez-vous que le niveau approprié de sécurisation renforcée vSphere est appliqué et maintenu.

Pour obtenir plus de conseils sur la sécurisation renforcée, consultez <http://www.vmware.com/security/hardening-guides.html>.

Dans le cadre d'un environnement entièrement renforcé, l'infrastructure VMware vSphere ® doit appliquer les directives de sécurité définies par VMware.

Sécurisation renforcée sur un hôte IaaS (Infrastructure en tant que service)

Assurez-vous que votre machine hôte IaaS (Infrastructure en tant que service) Microsoft Windows a été sécurisée de manière renforcée conformément aux directives de VMware.

Consultez les recommandations des directives de sécurisation renforcée et les meilleures pratiques de sécurité de Microsoft Windows, et assurez-vous que votre hôte Windows Server a bien été renforcé. La non-application des recommandations de sécurisation renforcée risque d'entraîner l'exposition à des failles de sécurité connues à partir de composants non sécurisés sur les différentes versions de Windows.

Pour vous assurer que votre version est prise en charge, reportez-vous à la [matrice de prise en charge de vRealize Automation](#).

Contactez votre fournisseur Microsoft pour en savoir plus sur les pratiques en matière de sécurisation renforcée des produits Microsoft.

Sécurisation renforcée de Microsoft SQL Server

Vérifiez que la base de données Microsoft SQL Server est conforme aux directives de sécurité fournies par Microsoft et par VMware.

Consultez les recommandations des directives en matière de sécurisation renforcée ainsi que les meilleures pratiques de sécurité de Microsoft SQL Server. Consultez tous les bulletins de sécurité Microsoft relatifs à la version installée de Microsoft SQL Server. La non-application des recommandations en matière de sécurisation renforcée risque d'entraîner l'exposition à des failles de sécurité connues à partir de composants non sécurisés sur les différentes versions de Microsoft SQL Server.

Pour vous assurer que votre version de Microsoft SQL Server est prise en charge, reportez-vous à la [matrice de prise en charge de vRealize Automation](#).

Contactez votre fournisseur Microsoft pour plus de détails sur les pratiques de sécurisation renforcée pour les produits Microsoft.

Sécurisation renforcée de Microsoft .NET

Dans le cadre d'un environnement entièrement renforcé, Microsoft .NET doit appliquer les directives de sécurité définies par Microsoft et par VMware.

Vérifiez les recommandations définies dans les directives sur la sécurisation renforcée et les meilleures pratiques de sécurité de .NET. En outre, consultez tous les bulletins de sécurité Microsoft concernant la version de Microsoft SQL Server que vous utilisez. La non-application des recommandations en matière de sécurisation renforcée risque d'entraîner l'exposition à des failles de sécurité connues à partir de composants Microsoft.NET non sécurisés.

Pour vous assurer que votre version de Microsoft.NET est prise en charge, reportez-vous à la [matrice de prise en charge de vRealize Automation](#).

Contactez votre fournisseur Microsoft pour plus de détails sur les pratiques de sécurisation renforcée concernant les produits Microsoft.

Sécurisation renforcée de Microsoft Internet Information Services (IIS)

Vérifiez que votre version de Microsoft Internet Information Services (IIS) est conforme à toutes les directives de sécurité de Microsoft et de VMware.

Vérifiez les recommandations figurant dans les directives de sécurisation renforcée et les meilleures pratiques de sécurité de Microsoft IIS. En outre, consultez tous les bulletins de sécurité Microsoft concernant la version d'IIS que vous utilisez. La non-application des recommandations en matière de sécurisation renforcée risque d'entraîner l'exposition à des failles de sécurité connues.

Pour vous assurer que votre version est prise en charge, reportez-vous à la [matrice de prise en charge de vRealize Automation](#).

Contactez votre fournisseur Microsoft pour plus de détails sur les pratiques de sécurisation renforcée concernant les produits Microsoft.

Vérification des logiciels installés

Dans la mesure où les vulnérabilités liées aux logiciels tiers et aux logiciels non utilisés augmentent le risque d'accès non autorisé au système et l'interruption de la disponibilité, il est

important de vérifier tous les logiciels installés sur les machines hôtes VMware et d'évaluer leur utilisation.

N'installez pas un logiciel qui ne soit pas nécessaire au fonctionnement sécurisé du système sur les machines hôtes VMware. Désinstallez les logiciels non utilisés ou superflus.

Inventaire des logiciels installés non pris en charge

Évaluez votre déploiement VMware et faites l'inventaire des produits installés pour vérifier qu'aucun logiciel non pris en charge n'est installé.

Pour plus d'informations sur les stratégies de prise en charge de produits tiers, reportez-vous à l'article d'assistance de VMware à la page : <https://www.vmware.com/support/policies/thirdparty.html>.

Vérification des logiciels tiers

VMware ne prend pas en charge et ne recommande pas l'installation des logiciels tiers qui n'ont pas été testés et vérifiés. Les logiciels tiers non sécurisés, sans correctifs ou non authentifiés installés sur des machines hôtes VMware, peuvent exposer le système à un accès non autorisé et perturber sa disponibilité. Si vous devez utiliser des logiciels tiers non pris en charge, consultez leurs éditeurs pour connaître les conditions requises pour la configuration sécurisée et l'application de correctifs.

Correctifs et avis de sécurité de VMware

Pour assurer une sécurité optimale de votre système, suivez les avis de sécurité de VMware et appliquez tous les correctifs appropriés.

VMware publie des avis de sécurité pour les produits. Informez-vous et tenez compte de ces avis pour vous assurer que votre produit est protégé contre les menaces connues.

Évaluez l'installation de vRealize Automation, l'application des correctifs et l'historique des mises à niveau, et vérifiez que les avis de sécurité publiés par VMware sont respectés et appliqués.

Pour plus d'informations sur les derniers avis de sécurité de VMware, consultez la page <http://www.vmware.com/security/advisories/>.

Configuration sécurisée

Vérifiez et mettez à jour les paramètres de sécurité des dispositifs virtuels vRealize Automation et du composant IaaS (Infrastructure en tant que service) en fonction de la configuration de votre système. En outre, vérifiez et mettez à jour la configuration des autres composants et applications.

La configuration sécurisée d'une installation vRealize Automation implique de traiter la configuration de chaque composant individuellement, en tenant compte de leurs interactions. Tenez compte de la configuration de tous les composants système pour obtenir une ligne de base raisonnablement sécurisée.

Sécurisation du dispositif vRealize Automation

Vérifiez et mettez à jour les paramètres de sécurité pour le dispositif vRealize Automation en fonction de la configuration de votre système.

Configurez les paramètres de sécurité pour vos dispositifs virtuels et leurs systèmes d'exploitation hôtes. En outre, définissez ou vérifiez la configuration d'autres applications et composants associés. Dans certains cas, vous devez vérifier les paramètres existants, alors que dans d'autres vous devez modifier ou ajouter des paramètres afin d'obtenir une configuration appropriée.

Modifier le mot de passe racine

Vous pouvez modifier le mot de passe racine du dispositif vRealize Automation.

Procédure

- 1 Connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Cliquez sur l'onglet **Admin**.
- 3 Cliquez sur le sous-menu **Admin**.
- 4 Entrez le mot de passe existant dans la zone de texte **Mot de passe d'administrateur actuel**.
- 5 Entrez le nouveau mot de passe dans la zone de texte **Nouveau mot de passe d'administrateur**.
- 6 Entrez le nouveau mot de passe dans la zone de texte **Confirmez le nouveau mot de passe d'administrateur**.
- 7 Cliquez sur **Enregistrer les paramètres**.

Vérifier le hachage et la complexité du mot de passe racine

Vérifiez que le mot de passe racine répond aux exigences de complexité des mots de passe d'entreprise de votre organisation.

La validation de la complexité du mot de passe racine est requise, car l'utilisateur racine contourne la vérification de la complexité du mot de passe du module pam_cracklib qui est appliquée aux comptes d'utilisateurs.

Le mot de passe de compte doit commencer par \$6\$, ce qui indique un hachage sha512. Il s'agit du hachage standard pour tous les dispositifs sécurisés.

Procédure

- 1 Pour vérifier le hachage du mot de passe racine, connectez-vous en tant qu'utilisateur racine et exécutez la commande `# more /etc/shadow`.

Les informations de hachage s'affichent.

Figure 1-1. Résultats du hachage de mot de passe

```
vcac148-084-111:~ $ more /etc/shadow
bin:!:16332:0:60:7:::
daemon:!:16332:0:60:7:::
haldaemon:!:16332:0:60:7:::
mail:!:15870::60:::
man:!:16332:0:60:7:::
messagebus:!:16332:0:60:7:::
nobody:!:15870::60:::
ntp:!:16332:0:60:7:::
polkituser:!:16332:0:60:7:::
postfix:!:16332:0:60:7:::
root:$6$PHxGPY5A$ba8KezK4SS44UEHPfAtgs
P/:16346:0:365:7:::
```

- 2 Si le mot de passe racine ne contient pas de hachage sha512, exécutez la commande `passwd` pour le modifier.

Résultats

Tous les dispositifs sécurisés activent `enforce_for_root` pour le module `pw_history`, disponible dans le fichier `/etc/pam.d/common-password`. Par défaut, le système mémorise les cinq derniers mots de passe. Les anciens mots de passe sont stockés pour chaque utilisateur dans le fichier `/etc/securetty/passwd`.

Vérifier l'historique du mot de passe racine

Vérifiez que l'historique du mot de passe est appliqué pour le compte racine.

Tous les dispositifs sécurisés activent `enforce_for_root` pour le module `pw_history`, disponible dans le fichier `/etc/pam.d/common-password`. Par défaut, le système mémorise les cinq derniers mots de passe. Les anciens mots de passe sont stockés pour chaque utilisateur dans le fichier `/etc/securetty/passwd`.

Procédure

- 1 Exécutez la commande suivante :


```
cat /etc/pam.d/common-password-vmware.local | grep pam_pwhistory.so
```
- 2 Assurez-vous que `enforce_for_root` apparaît dans les résultats renvoyés.


```
password required pam_pwhistory.so enforce_for_root remember=5 retry=3
```

Gérer l'expiration des mots de passe

Configurez toutes les expirations de mot de passe des comptes conformément aux stratégies de sécurité de votre organisation.

Par défaut, tous les comptes du dispositif virtuel VMware renforcé appliquent un délai d'expiration de mot de passe de 60 jours. Sur la plupart des dispositifs renforcés, l'expiration de mot de passe du compte racine est fixée à 365 jours. Il est recommandé de vérifier que la date d'expiration de l'ensemble des comptes répond aux normes de sécurité et d'opération.

Si le mot de passe racine expire, vous ne pouvez pas le rétablir. Vous devez implémenter des stratégies propres au site pour éviter l'expiration des mots de passe d'administration et racines.

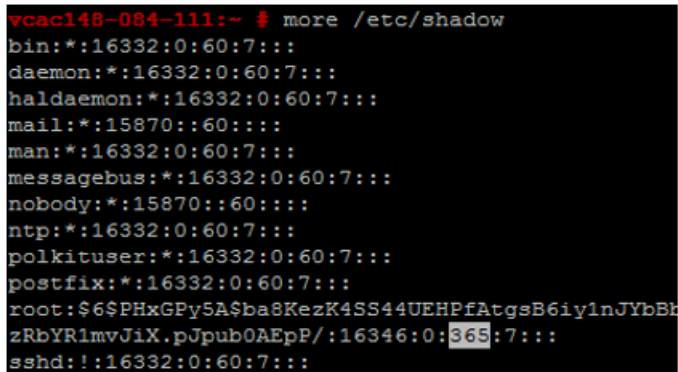
Procédure

- 1 Connectez-vous aux machines du dispositif virtuel en tant qu'utilisateur racine et exécutez la commande suivante pour vérifier la date d'expiration des mots de passe sur tous les comptes.

```
# cat /etc/shadow
```

Les informations d'expiration du mot de passe figurent dans le cinquième champ (les champs sont séparés par le signe deux-points) du fichier caché. L'expiration du mot de passe racine est définie en jours.

Figure 1-2. Champ de date d'expiration de mot de passe



```
vcac148-084-111:~ # more /etc/shadow
bin:!:16332:0:60:7:::
daemon:!:16332:0:60:7:::
haldaemon:!:16332:0:60:7:::
mail:!:15870::60:::
man:!:16332:0:60:7:::
messagebus:!:16332:0:60:7:::
nobody:!:15870::60:::
ntp:!:16332:0:60:7:::
polkituser:!:16332:0:60:7:::
postfix:!:16332:0:60:7:::
root:$6$PHxGPY5A$ba8KczK4SS44UEHPfAtgsB6iy1nJYbBh
zRbYR1mvJiX.pJpub0AEpP/:16346:0:365:7:::
sshd:!:16332:0:60:7:::
```

- 2 Pour modifier le délai d'expiration du compte racine, exécutez une commande au format suivant :

```
# passwd -x 365 root
```

Dans cette commande, 365 indique le nombre de jours jusqu'à l'expiration du mot de passe. Utilisez la même commande pour modifier n'importe quel utilisateur, en remplaçant le compte concerné par « racine » et en remplaçant le nombre de jours conformément aux normes d'expiration de l'organisation.

Gestion de comptes administratifs et Secure Shell (SSH)

Pour les connexions à distance, tous les dispositifs renforcés incluent le protocole SSH (Secure Shell). Utilisez uniquement le protocole SSH lorsque cela est nécessaire et gérez-le de façon à préserver la sécurité du système.

SSH est un environnement interactif de ligne de commande qui prend en charge les connexions à distance aux dispositifs virtuels VMware. Par défaut, l'accès SSH nécessite des informations d'identification de compte d'utilisateur avec des privilèges élevés. Les activités SSH de l'utilisateur racine contournent généralement le contrôle d'accès basé sur les rôles (RBAC) et les audits des dispositifs virtuels.

Il est recommandé de désactiver le mode SSH dans un environnement de production et de l'activer uniquement pour résoudre les problèmes que vous ne pouvez pas résoudre par d'autres moyens. Cette option doit rester activée uniquement pour des objectifs spécifiques et conformément aux stratégies de sécurité de votre organisation. Le mode SSH est désactivé par défaut sur le dispositif vRealize Automation. Selon votre configuration vSphere, vous pouvez activer ou désactiver le mode SSH lors du déploiement du modèle OVF (Open Virtualization Format).

Pour opérer un test simple et déterminer si le mode SSH est activé sur une machine, essayez d'ouvrir une connexion via SSH. Si la connexion s'ouvre et que des informations d'identification sont demandées, le mode SSH est activé et disponible pour les connexions.

Compte d'utilisateur racine SSH (Secure Shell)

Les dispositifs VMware n'incluant pas de comptes d'utilisateur préconfigurés, le compte racine peut utiliser le mode SSH pour se connecter directement par défaut. Désactivez le mode SSH en tant qu'utilisateur racine dès que possible.

À des fins de conformité avec les normes de non-répudiation, le serveur SSH de tous les dispositifs renforcés est préconfiguré avec l'entrée du groupe wheel AllowGroups pour limiter l'accès SSH au groupe secondaire (wheel). Pour séparer les tâches, vous pouvez modifier le champ AllowGroups du groupe wheel dans le fichier `/etc/ssh/sshd_config` pour utiliser un autre groupe tel que `sshd`.

Le groupe wheel est activé avec le module `pam_wheel` pour l'accès superutilisateur, ce qui permet aux membres du groupe wheel d'utiliser `su-root`, où le mot de passe racine est requis. La séparation des groupes permet aux utilisateurs d'utiliser le mode SSH pour le dispositif, mais pas d'utiliser le script `su-to-root`. Ne supprimez ni ne modifiez aucune autre entrée dans le champ AllowGroups, afin d'assurer le bon fonctionnement du dispositif. Une fois la modification effectuée, redémarrez le démon SSH en exécutant la commande suivante : `# service sshd restart`.

Activer ou désactiver le protocole SSH (Secure Shell) sur les dispositifs vRealize Automation

Activez le protocole SSH (Secure Shell) sur le dispositif vRealize Automation uniquement à des fins de dépannage. Désactivez le mode SSH sur ces composants au cours des opérations normales de production.

Vous pouvez activer ou désactiver le protocole SSH sur le dispositif vRealize Automation au moyen de l'interface de gestion du dispositif vRealize Automation.

Procédure

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

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

- 2 Cliquez sur l'onglet **Admin**.
- 3 Cliquez sur le sous-menu **Admin**.

- 4 Activez la case **Activer le service SSH** pour activer le mode SSH ou désactivez-la pour le désactiver.
- 5 Cliquez sur **Enregistrer les paramètres** pour enregistrer les modifications.

Créer un compte d'administrateur local pour Secure Shell

Pour garantir la sécurité, il est recommandé de créer et de configurer des comptes administratifs locaux pour Secure Shell (SSH) sur vos machines hôtes de dispositif virtuel. En outre, supprimez l'accès SSH racine après la création des comptes appropriés.

Créez des comptes administratifs locaux pour SSH ou pour les membres du groupe wheel secondaire, ou pour les deux. Avant de désactiver un accès racine direct, vérifiez que les administrateurs autorisés peuvent accéder à SSH à l'aide d'AllowGroups, et qu'ils peuvent utiliser l'accès su-to-root avec le groupe wheel.

Procédure

- 1 Connectez-vous au dispositif virtuel en tant qu'utilisateur racine et exécutez les commandes suivantes avec le nom d'utilisateur approprié.

```
# useradd -g users <username> -G wheel -m -d /home/username
# passwd username
```

Wheel est le groupe spécifié dans AllowGroups pour les accès SSH. Pour ajouter plusieurs groupes secondaires, utilisez `-G wheel,sshd`.

- 2 Fournissez ensuite un nouveau mot de passe pour l'utilisateur afin d'appliquer la vérification de la complexité du mot de passe.

```
# su -username
# username@hostname:~>passwd
```

Si la complexité du mot de passe est conforme, le mot de passe est mis à jour. Si la complexité du mot de passe n'est pas conforme, le mot de passe d'origine est rétabli et vous devez relancer la commande de mot de passe.

- 3 Pour supprimer une connexion directe à SSH, modifiez le fichier `/etc/ssh/sshd_config` en remplaçant `(#)PermitRootLogin yes` par `PermitRootLogin no`.

Vous pouvez également activer ou désactiver SSH dans l'interface VAMI (Virtual Appliance Management Interface) en activant ou en désactivant la case **Connexion SSH de l'administrateur activée** dans l'onglet **Admin**.

Étape suivante

Désactivez les connexions directes en tant qu'utilisateur racine. Par défaut, les dispositifs renforcés autorisent une connexion directe à la racine via la console. Une fois que vous avez créé des comptes administratifs pour la non-répudiation et que vous les avez testés pour un accès wheel su-root, désactivez les connexions racines directes en modifiant le fichier `/etc/security` en tant qu'utilisateur racine et en remplaçant l'entrée `tty1` par `console`.

- 1 Ouvrez le fichier `/etc/securetty` dans un éditeur de texte.
- 2 Localisez `tty1` et remplacez-le par `console`.
- 3 Enregistrez le fichier et fermez-le.

Renforcer la configuration du serveur Secure Shell

Dans la mesure du possible, tous les dispositifs VMware doivent disposer d'une configuration sécurisée de manière renforcée par défaut. Les utilisateurs peuvent vérifier que leur configuration est suffisamment renforcée en examinant les paramètres des services serveur et client dans la section des options globales du fichier de configuration.

Procédure

- 1 Ouvrez le fichier de configuration de serveur `/etc/ssh/sshd_config` sur le dispositif VMware et vérifiez que les paramètres sont corrects.

Configuration	État
Protocole démon du serveur	Protocole 2
Chiffrements CBC	aes256-ctr et aes128-ctr
Transfert TCP	AllowTCPForwarding no
Ports de passerelle serveur	GatewayPorts no
Transfert X11	X11Forwarding no
Service SSH	Utilisez le champ <code>AllowGroups</code> pour spécifier une autorisation d'accès pour le groupe. Ajoutez des membres appropriés à ce groupe.
Authentification GSSAPI	GSSAPIAuthentication no (si non utilisé)
Authentification Keberos	KeberosAuthentication no (si non utilisé)
Variables locales (option globale <code>AcceptEnv</code>)	Définissez ces variables sur <code>disabled by commenting out</code> ou sur <code>enabled for LC_* or LANG variables</code> .
Configuration de tunnel	PermitTunnel no
Sessions réseau	MaxSessions 1
Connexions simultanées de l'utilisateur	Définissez cette valeur sur 1 pour l'utilisateur racine et tout autre utilisateur. Le fichier <code>/etc/security/limits.conf</code> doit également être configuré avec le même paramètre.
Vérification en mode strict	StrictModes yes

Configuration	État
Séparation des privilèges	UsePrivilegeSeparation yes
Authentification RSA rhosts	RhostsESAAuthentication no
Compression	Compression delayed ou Compression no
Code d'authentification de message	MACs hmac-sha1
Limitation d'accès utilisateur	PermitUserEnvironment no

2 Enregistrez les modifications et fermez le fichier.

Renforcer la configuration du client SSH (Secure Shell)

Dans le cadre de la sécurisation renforcée du système, vérifiez la sécurisation renforcée du client SSH en examinant le fichier de configuration du client SSH sur les machines hôtes du dispositif virtuel, afin de vous assurer que la configuration est conforme aux directives de VMware.

Procédure

- 1 Ouvrez le fichier de configuration du client SSH (/etc/ssh/ssh_config) et vérifiez que les paramètres de la section des options globales sont corrects.

Configuration	État
Protocole du client	Protocole 2
Ports de la passerelle du client	GatewayPorts no
Authentification GSSAPI	GSSAPIAuthentication no
Variables locales (option globale SendEnv)	Variables LC_* ou LANG uniquement
Chiffrements CBC	aes256-ctr et aes128-ctr uniquement
Codes d'authentification de message	Utilisés pour l'entrée MACs hmac-sha1 uniquement

2 Enregistrez les modifications et fermez le fichier.

Vérification des autorisations de fichier de clé Secure Shell

Afin de minimiser les risques d'attaques malveillantes, gérez les autorisations de fichier de clé SSH critiques sur les machines hôtes du dispositif virtuel.

Après la configuration ou la mise à jour de votre configuration SSH, vérifiez toujours que les autorisations de fichier de clé SSH suivantes restent inchangées.

- Les fichiers de clé hôte publique situés dans /etc/ssh/*key.pub appartiennent à l'utilisateur racine et disposent d'autorisations définies sur 0644 (-rw-r--r--).
- Les fichiers de clé hôte privée situés dans /etc/ssh/*key appartiennent à l'utilisateur racine et disposent d'autorisations définies sur 0600 (-rw-----).

Vérifier les autorisations de fichier de clés SSH

Assurez-vous que les autorisations SSH sont appliquées aux fichiers de clés publiques et de clés privées.

Procédure

- 1 Vérifiez les fichiers de clés publiques SSH en exécutant la commande suivante : `ls -l /etc/ssh/*key.pub`
- 2 Assurez-vous que le propriétaire est de type racine, que le propriétaire du groupe est de type racine et que les autorisations des fichiers sont définies sur 0644 (-rw-r--r--).
- 3 Corrigez les problèmes en exécutant les commandes suivantes.


```
chown root /etc/ssh/*key.pub
chgrp root /etc/ssh/*key.pub
chmod 644 /etc/ssh/*key.pub
```
- 4 Vérifiez les fichiers de clés privées SSH en exécutant la commande suivante : `ls -l /etc/ssh/*key`
- 5 Assurez-vous que le propriétaire est de type racine, que le propriétaire du groupe est de type racine et que les autorisations des fichiers sont définies sur 0600 (-rw-----). Corrigez les problèmes en exécutant les commandes suivantes.


```
chown root /etc/ssh/*key
chgrp root /etc/ssh/*key
chmod 600 /etc/ssh/*key
```

Modifier l'utilisateur de l'interface de gestion de dispositif virtuel

Vous pouvez ajouter et supprimer des utilisateurs sur l'interface de gestion de dispositif virtuel pour créer le niveau approprié de sécurité.

Le compte d'utilisateur racine pour l'interface de gestion de dispositif virtuel utilise PAM pour l'authentification, donc les niveaux de coupure définis par PAM s'appliquent également. Si vous n'avez pas correctement isolé l'interface de gestion de dispositif virtuel, un verrouillage du compte racine système peut se produire si un pirate tente de forcer la connexion. En outre, lorsque le compte racine est considéré comme insuffisant pour fournir la non-répudiation par plusieurs personnes de votre organisation, vous pouvez décider de modifier l'utilisateur Admin de l'interface de gestion.

Conditions préalables

Procédure

- 1 Exécutez la commande suivante pour créer un nouvel utilisateur et l'ajouter au groupe d'interface de gestion de dispositif virtuel.


```
useradd -G vami,root user
```


- 2 Créez un mot de passe pour l'utilisateur.

```
passwd user
```

- 3 (Facultatif) Exécutez la commande suivante pour désactiver l'accès racine à l'interface de gestion de dispositif virtuel.

```
usermod -R vami root
```

Note La désactivation d'un accès racine à l'interface de gestion de dispositif virtuel désactive également la possibilité de mettre à jour le mot de passe de l'administrateur, ou le mot de passe racine, dans l'onglet Admin.

Définir l'authentification du chargeur de démarrage

Pour fournir un niveau de sécurité adapté, configurez l'authentification du chargeur de démarrage sur vos dispositifs virtuels VMware.

Si le chargeur de démarrage du système ne requiert aucune authentification, les utilisateurs ayant accès à la console système peuvent modifier la configuration de démarrage du système ou démarrer le système en mode mono-utilisateur unique ou en mode de maintenance, ce qui peut entraîner un déni de service ou un accès système non autorisé. Étant donné que l'authentification du chargeur de démarrage n'est pas définie par défaut sur les dispositifs virtuels VMware, vous devez créer un mot de passe GRUB pour la configurer.

Procédure

- 1 Vérifiez si un mot de passe de démarrage existe en localisant la ligne `password --md5 <password-hash>` dans le fichier `/boot/grub/menu.lst` sur les dispositifs virtuels.
- 2 S'il n'existe aucun mot de passe, exécutez la commande `# /usr/sbin/grub-md5-crypt` sur votre dispositif virtuel.

Un mot de passe MD5 est généré et la commande fournit la sortie de hachage md5.

- 3 Ajoutez le mot de passe au fichier `menu.lst` en exécutant la commande `# password --md5 <hash from grub-md5-crypt>`.

Configurer NTP

Pour les sources d'heure critiques, désactivez la synchronisation date/heure de l'hôte et utilisez le protocole NTP (Network Time Protocol) sur le dispositif vRealize Automation.

Le démon NTP sur le dispositif vRealize Automation fournit des services de synchronisation d'heure. Le protocole NTP est désactivé par défaut. Vous devez donc le configurer manuellement. Si possible, utilisez NTP dans des environnements de production pour effectuer le suivi des actions des utilisateurs et pour détecter d'éventuelles attaques malveillantes et intrusions au moyen d'un audit et d'une journalisation détaillés. Pour plus d'informations sur les avis de sécurité NTP, consultez le site Web NTP.

Le fichier de configuration NTP est situé dans le dossier `/etc/` sur chaque dispositif. Vous pouvez activer le service NTP pour le dispositif vRealize Automation et ajouter des serveurs de temps dans l'onglet **Admin** de l'interface VAMI.

Procédure

- 1 Ouvrez le fichier de configuration `/etc/ntp.conf` sur la machine hôte de votre dispositif virtuel dans un éditeur de texte.
- 2 Définissez la propriété de fichier sur **root:root**.
- 3 Définissez les autorisations sur **0640**.
- 4 Pour réduire les risques d'une attaque par déni de service avec technique d'amplification sur le service NTP, ouvrez le fichier `/etc/ntp.conf` et assurez-vous que les lignes `restrict` figurent dans le fichier.

```
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict -6 ::1
```

- 5 Enregistrez les modifications et fermez les fichiers.

Configuration du protocole TLS pour les données en transit du dispositif vRealize Automation

Assurez-vous que votre déploiement vRealize Automation utilise des protocoles TLS forts afin de sécuriser les canaux de transmission pour les composants du dispositif vRealize Automation.

Pour ne pas compromettre les performances, le protocole TLS n'est pas activé pour les connexions localhost entre certains services d'application. Lorsqu'une défense poussée est requise, activez TLS sur toutes les communications localhost.

Important Si vous arrêtez TLS sur l'équilibrage de charge, désactivez les protocoles non sécurisés tels que SSLv2, SSLv3 et TLS 1.0 sur tous les équilibres de charge.

Activer TLS sur une configuration localhost

Par défaut, certaines communications localhost n'utilisent pas TLS. Vous pouvez activer TLS sur l'ensemble des connexions localhost pour assurer une sécurité renforcée.

Procédure

- 1 Connectez-vous au dispositif vRealize Automation au moyen du mode SSH.
- 2 Définissez des autorisations pour le keystore vCAC en exécutant les commandes suivantes.

```
usermod -A vco,coredump,pivotal vco
chown vcac.pivotal /etc/vcac/vcac.keystore
chmod 640 /etc/vcac/vcac.keystore
```

3 Mettez à jour la configuration de HAProxy.

- a Ouvrez le fichier de configuration HAProxy situé dans `/etc/haproxy/conf.d` et choisissez le service `vcac.cfg-20`.

- b Recherchez les lignes contenant la chaîne suivante :

`server local 127.0.0.1...` et ajoutez la ligne suivante à la fin de ces lignes : `ssl verify none`

Cette section contient également d'autres lignes :

<code>backend-horizon</code>	<code>backend-vro</code>
<code>backend-vra</code>	<code>backend-artifactory</code>
<code>backend-vra-health</code>	

- c Pour `backend-horizon`, remplacez le port 8080 par 8443.

4 Obtenez le mot de passe de keystorePass.

- a Recherchez la propriété `certificate.store.password` dans le fichier `/etc/vcac/security.properties`.

Par exemple, `certificate.store.password=s2enc~iom0GXATG+RB8ff7Wdm4Bg==`.

- b Déchiffrez la valeur au moyen de la commande suivante :

`vcac-config prop-util -d --p VALUE`

Par exemple, `vcac-config prop-util -d --p s2enc~iom0GXATG+RB8ff7Wdm4Bg==`.

5 Configurez le service vRealize Automation.

- a Ouvrez le fichier `/etc/vcac/server.xml`.
- b Ajoutez l'attribut suivant à la balise de connecteur, en remplaçant `certificate.store.password` par la valeur du mot de passe de magasin de certificats figurant dans `etc/vcac/security.properties`.

```
scheme="https" secure="true" SSLEnabled="true" sslProtocol="TLS" keystoreFile="/etc/vcac/vcac.keystore" keyAlias="apache" keystorePass="certificate.store.password"
```

6 Configurez le service vRealize Orchestrator.

- a Ouvrez le fichier `/etc/vco/app-server.xml`
- b Ajoutez l'attribut suivant à la balise de connecteur, en remplaçant `certificate.store.password` par la valeur du mot de passe de magasin de certificats figurant dans `etc/vcac/security.properties`.

```
scheme="https" secure="true" SSLEnabled="true" sslProtocol="TLS" keystoreFile="/etc/vcac/vcac.keystore" keyAlias="apache" keystorePass="certificate.store.password"
```

7 Redémarrez les services vRealize Orchestrator, vRealize Automation et HAProxy.

```
service vcac-server restart
service vco-server restart
service haproxy restart
```

Note Si le serveur vCO ne redémarre pas, redémarrez l'ordinateur hôte.

8 Configurez l'interface VAMI (Virtual Appliance Management Interface).

Vous pouvez afficher l'état des services en exécutant la commande suivante sur le dispositif virtuel vRealize Automation.

```
curl -ks -H "Content-Type: application/json" https://localhost/component-registry/services/status/
current?limit=200 | jq -re '.content[]|\"(.serviceStatus.serviceName) \
(.serviceStatus.serviceInitializationStatus)\"'
```

Note Si vous activez SSL sur l'interface de gestion du dispositif virtuel, l'onglet Services ne peut pas indiquer l'état des services vRealize Automation.

- a Ouvrez le fichier `/opt/vmware/share/htdocs/service/café-services/services.py`.
- b Remplacez la ligne `conn = httplib.HTTP()` par `conn = httplib.HTTPS()` pour renforcer la sécurité.

Activer la conformité FIPS (Federal Information Processing Standard) 140-2

Le dispositif vRealize Automation utilise désormais la version certifiée Federal Information Processing Standard (FIPS) 140-2 d'OpenSSL pour les données en transit via TLS sur tout le trafic réseau, entrant et sortant.

Vous pouvez activer ou désactiver le mode FIPS dans l'interface de gestion du dispositif vRealize Automation. Vous pouvez également configurer le mode FIPS à partir de la ligne de commande lorsque vous êtes connecté en tant qu'utilisateur racine, au moyen des commandes suivantes :

```
vcac-vami fips enable
vcac-vami fips disable
vcac-vami fips status
```

Lorsque le mode FIPS est activé, le trafic réseau entrant et sortant du dispositif vRealize Automation sur le port 443 applique le chiffrement conforme à la norme FIPS 140-2. Quel que soit le paramètre FIPS, vRealize Automation applique la norme AES-256 pour protéger les données sécurisées stockées sur le dispositif vRealize Automation.

Note Actuellement, vRealize Automation assure une conformité FIPS partielle, car certains composants internes n'utilisent pas encore de modules de chiffrement certifiés. Si des modules certifiés n'ont pas encore été implémentés, le chiffrement AES-256 est utilisé par tous les algorithmes de chiffrement.

Note La procédure suivante fait redémarrer la machine physique lorsque vous modifiez la configuration.

Procédure

- 1 Connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Sélectionnez **vRA > Paramètres de l'hôte**.
- 3 Cliquez sur le bouton situé sous l'en-tête Actions dans la partie supérieure droite pour activer ou désactiver le mode FIPS.
- 4 Cliquez sur **Oui** pour redémarrer le dispositif vRealize Automation

Vérifier que les protocoles SSLv3, TLS 1.0 et TLS 1.1 sont désactivés

Dans le cadre du processus de sécurisation renforcée, assurez-vous que le dispositif vRealize Automation déployé utilise des canaux de transmission sécurisés.

Note Vous ne pouvez pas exécuter l'opération Joindre un cluster après la désactivation de TLS 1.0/1.1 et l'activation de TLS 1.2

Conditions préalables

Effectuez [Activer TLS sur une configuration localhost](#).

Procédure

- 1 Vérifiez que les protocoles TLS 1.1, TLS 1.0 et SSLv3 sont désactivés dans les gestionnaires https HAProxy sur dispositif vRealize Automation.

Fichier à examiner	Vérifier la présence de ces éléments	Sur la ligne appropriée, comme indiqué
/etc/haproxy/conf.d/20-vcac.cfg	no-sslv3 no-tlsv10 no-tls11 force-tls12	bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-sslv3 no-tlsv10 no-tls11
/etc/haproxy/conf.d/30-vro-config.cfg	no-sslv3 no-tlsv10 no-tls11 force-tls12	bind :::8283 v4v6 ssl crt /opt/vmware/etc/lighttpd/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-sslv3 no-tlsv10 no-tls11

- 2 Redémarrez le service.

```
service haproxy restart
```

- 3 Ouvrez le fichier `/opt/vmware/etc/lighttpd/lighttpd.conf` et vérifiez que les entrées désactivées correctes s'affichent.

Note Aucune directive n'impose la désactivation de TLS 1.0 ou TLS 1.1 dans Lighttpd. Vous pouvez atténuer partiellement la restriction d'utilisation de TLS 1.0 et TLS 1.1 en appliquant OpenSSL afin de ne pas utiliser les suites de chiffrement de TLS 1.0 et TLS 1.1.

```
ssl.use-ssl2 = "disable"
ssl.use-ssl3 = "disable"
```

- 4 Vérifiez que les protocoles SSLv3, TLS 1.0 et TLS 1.1 sont désactivés pour le proxy de la console sur dispositif vRealize Automation.
 - a Modifiez le fichier `/etc/vcac/security.properties` en ajoutant ou en modifiant la ligne suivante :


```
consoleproxy.ssl.server.protocols = TLSv1.2
```
 - b Redémarrez le serveur en exécutant la commande suivante :


```
service vcac-server restart
```
- 5 Vérifiez que les protocoles SSLv3, TLS 1.0 et TLS 1.1 sont désactivés pour le service vCO.
 - a Localisez la balise `<Connector>` dans le fichier `/etc/vco/app-server/server.xml` et ajoutez l'attribut suivant :


```
sslEnabledProtocols = "TLSv1.2"
```
 - b Redémarrez le service vCO en exécutant la commande suivante.


```
service vco-server restart
```
- 6 Vérifiez que les protocoles SSLv3, TLS 1.0 et TLS 1.1 sont désactivés pour le service vRealize Automation.
 - a Ajoutez les attributs suivants à la balise `<Connector>` dans le fichier `/etc/vcac/server.xml`.


```
sslEnabledProtocols = "TLSv1.2"
```
 - b Redémarrez le service vRealize Automation en exécutant la commande suivante :


```
service vcac-server restart
```
- 7 Vérifiez que les protocoles SSLv3, TLS 1.0 et TLS 1.1 sont désactivés pour RabbitMQ.

Ouvrez le fichier `/etc/rabbitmq/rabbitmq.config` et vérifiez que seul `{versions, ['tlsv1.2']}` est présent dans les sections `ssl` et `ssl_options`.

```
[
  {ssl, [
    {versions, ['tlsv1.2']},
    {ciphers, ["AES256-SHA", "AES128-SHA"]}
  ]},
  {rabbit, [
    {tcp_listeners, [{"127.0.0.1", 5672}]}
  ]}
```

```

    {frame_max, 262144},
    {ssl_listeners, [5671]},
    {ssl_options, [
      {cacertfile, "/etc/rabbitmq/certs/ca/cacert.pem"},
      {certfile, "/etc/rabbitmq/certs/server/cert.pem"},
      {keyfile, "/etc/rabbitmq/certs/server/key.pem"},
      {versions, ['tlsv1.2']},
      {ciphers, ["AES256-SHA", "AES128-SHA"]},
      {verify, verify_peer},
      {fail_if_no_peer_cert, false}
    ]},
    {mnesia_table_loading_timeout, 600000},
    {cluster_partition_handling, autoheal},
    {heartbeat, 600}
  ]},
  {kernel, [{net_ticktime, 120}]}
].

```

8 Redémarrez le serveur RabbitMQ.

```
# service rabbitmq-server restart
```

9 Vérifiez que les protocoles SSLv3, TLS 1.0 et TLS 1.1 sont désactivés pour le service vIDM.

Ouvrez le fichier `opt/vmware/horizon/workspace/conf/server.xml` pour chaque instance du connecteur contenant `SSLEnabled="true"` et assurez-vous que la ligne suivante est présente.

```
ssLEnabledProtocols="TLSv1.2"
```

Configuration des suites de chiffrement TLS pour les composants vRealize Automation

Pour obtenir une sécurité maximale, vous devez configurer les composants vRealize Automation pour utiliser des chiffrements forts.

Le chiffrement négocié entre le serveur et le navigateur détermine la force du chiffrement utilisé dans une session TLS.

Pour vous assurer que seuls des chiffrements forts sont sélectionnés, désactivez les chiffrements faibles dans les composants vRealize Automation. Configurez le serveur pour prendre en charge uniquement les chiffrements forts et pour utiliser des clés suffisamment grandes. En outre, configurez tous les chiffrements dans l'ordre approprié.

Désactivez les suites de chiffrement qui ne proposent pas d'authentification telles que les suites de chiffrement NULL, aNULL ou eNULL. Désactivez également l'échange de clés anonyme Diffie-Hellman (ADH), les chiffrements de niveau exportation (EXP, chiffrements contenant des algorithmes DES), les tailles de clé inférieures à 128 bits pour le chiffrement du trafic de la charge utile, l'utilisation de la fonction MD5 comme mécanisme de hachage pour le trafic de charge utile, les suites de chiffrement IDEA et les suites de chiffrement RC4. Assurez-vous également que les suites de chiffrement utilisant l'échange de clés Diffie-Hellman (DHE) sont désactivées.

Pour plus d'informations sur la désactivation de TLS, reportez-vous à [l'article 2146570 de la base de connaissances](#).

Désactiver les chiffrements faibles dans HAProxy

Vérifiez les chiffrements du service HA proxy du dispositif vRealize Automation par rapport à la liste de chiffrements acceptables et désactivez tous ceux qui sont considérés comme faibles.

Désactivez les suites de chiffrement qui ne proposent pas d'authentification telles que les suites de chiffrement NULL, aNULL ou eNULL. Désactivez également l'échange de clés anonyme Diffie-Hellman (ADH), les chiffrements de niveau exportation (EXP, chiffrements contenant des algorithmes DES), les tailles de clé inférieures à 128 bits pour le chiffrement du trafic de la charge utile, l'utilisation de la fonction MD5 comme mécanisme de hachage pour le trafic de charge utile, les suites de chiffrement IDEA et les suites de chiffrement RC4.

Procédure

- 1 Vérifiez les entrées de chiffrement du fichier `/etc/haproxy/conf.d/20-vcac.cfg` de la directive de liaison et désactivez ceux qui sont considérés comme faibles.

```
bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-ssl3 no-tls10 no-tls11
```

- 2 Vérifiez les entrées de chiffrement du fichier `/etc/haproxy/conf.d/30-vro-config.cfg` de la directive de liaison et désactivez ceux qui sont considérés comme faibles.

```
bind :::8283 v4v6 ssl crt /opt/vmware/etc/lighttpd/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-ssl3 no-tls10 no-tls11
```

Désactiver les chiffrements faibles dans le service de proxy de console du dispositif vRealize Automation

Vérifiez les chiffrements du service de proxy de console du dispositif vRealize Automation par rapport à la liste de chiffrements acceptables et désactivez tous ceux qui sont considérés comme faibles.

Désactivez les suites de chiffrement qui ne proposent pas d'authentification telles que les suites de chiffrement NULL, aNULL ou eNULL. Désactivez également l'échange de clés anonyme Diffie-Hellman (ADH), les chiffrements de niveau exportation (EXP, chiffrements contenant des algorithmes DES), les tailles de clé inférieures à 128 bits pour le chiffrement du trafic de la charge utile, l'utilisation de la fonction MD5 comme mécanisme de hachage pour le trafic de charge utile, les suites de chiffrement IDEA et les suites de chiffrement RC4.

Procédure

- 1 Ouvrez le fichier `/etc/vcac/security.properties` dans un éditeur de texte.
- 2 Ajoutez une ligne dans le fichier pour désactiver les suites de chiffrement indésirables.

Utilisez une variante de la ligne suivante :

```
consoleproxy.ssl.ciphers.disallowed=cipher_suite_1, cipher_suite_2,etc
```


Par exemple, pour désactiver les suites de chiffrement AES 128 et AES 256, ajoutez la ligne suivante :

```
consoleproxy.ssl.ciphers.disallowed=TLS_DH_DSS_WITH_AES_128_CBC_SHA,
TLS_DH_DSS_WITH_AES_256_CBC_SHA, TLS_DH_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

- 3 Redémarrez le serveur à l'aide de la commande suivante.

```
service vcac-server restart
```

Désactiver les chiffrements faibles dans le service vCO de dispositif vRealize Automation
Vérifiez les chiffrements du service vCO de dispositif vRealize Automation par rapport à la liste de chiffrements acceptables et désactivez tous ceux qui sont considérés comme faibles.

Désactivez les suites de chiffrement qui ne proposent pas d'authentification telles que les suites de chiffrement NULL, aNULL ou eNULL. Désactivez également l'échange de clés anonyme Diffie-Hellman (ADH), les chiffrements de niveau exportation (EXP, chiffrements contenant des algorithmes DES), les tailles de clé inférieures à 128 bits pour le chiffrement du trafic de la charge utile, l'utilisation de la fonction MD5 comme mécanisme de hachage pour le trafic de charge utile, les suites de chiffrement IDEA et les suites de chiffrement RC4.

Procédure

- 1 Recherchez la balise <Connector> dans le fichier /etc/vco/app-server/server.xml.
- 2 Modifiez ou ajoutez l'attribut de chiffrement pour utiliser les suites de chiffrement souhaitées.

Reportez-vous à l'exemple suivant :

```
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
```

Désactiver les chiffrements faibles dans le service RabbitMQ de dispositif vRealize Automation
Vérifiez le chiffrement du service RabbitMQ de dispositif vRealize Automation par rapport à la liste de chiffrements acceptables et désactivez tous ceux qui sont considérés comme faibles.

Désactivez les suites de chiffrement qui ne proposent pas d'authentification telles que les suites de chiffrement NULL, aNULL ou eNULL. Désactivez également l'échange de clés anonyme Diffie-Hellman (ADH), les chiffrements de niveau exportation (EXP, chiffrements contenant des algorithmes DES), les tailles de clé inférieures à 128 bits pour le chiffrement du trafic de la charge utile, l'utilisation de la fonction MD5 comme mécanisme de hachage pour le trafic de charge utile, les suites de chiffrement IDEA et les suites de chiffrement RC4.

Procédure

- 1 Évaluez les suites de chiffrement prises en charge en exécutant la commande `# /usr/sbin/rabbitmqctl eval 'ssl:cipher_suites()'`.

Les chiffrements renvoyés dans l'exemple suivant représentent uniquement les chiffrements pris en charge. Le serveur RabbitMQ n'utilise, ni n'annonce ces chiffrements, sauf si la configuration spécifiée dans le fichier `rabbitmq.config` l'autorise.

```
[ "ECDHE-ECDSA-AES256-GCM-SHA384", "ECDHE-RSA-AES256-GCM-SHA384",
  "ECDHE-ECDSA-AES256-SHA384", "ECDHE-RSA-AES256-SHA384",
  "ECDH-ECDSA-AES256-GCM-SHA384", "ECDH-RSA-AES256-GCM-SHA384",
  "ECDH-ECDSA-AES256-SHA384", "ECDH-RSA-AES256-SHA384",
  "DHE-RSA-AES256-GCM-SHA384", "DHE-DSS-AES256-GCM-SHA384",
  "DHE-RSA-AES256-SHA256", "DHE-DSS-AES256-SHA256", "AES256-GCM-SHA384",
  "AES256-SHA256", "ECDHE-ECDSA-AES128-GCM-SHA256",
  "ECDHE-RSA-AES128-GCM-SHA256", "ECDHE-ECDSA-AES128-SHA256",
  "ECDHE-RSA-AES128-SHA256", "ECDH-ECDSA-AES128-GCM-SHA256",
  "ECDH-RSA-AES128-GCM-SHA256", "ECDH-ECDSA-AES128-SHA256",
  "ECDH-RSA-AES128-SHA256", "DHE-RSA-AES128-GCM-SHA256",
  "DHE-DSS-AES128-GCM-SHA256", "DHE-RSA-AES128-SHA256", "DHE-DSS-AES128-SHA256",
  "AES128-GCM-SHA256", "AES128-SHA256", "ECDHE-ECDSA-AES256-SHA",
  "ECDHE-RSA-AES256-SHA", "DHE-RSA-AES256-SHA", "DHE-DSS-AES256-SHA",
  "ECDH-ECDSA-AES256-SHA", "ECDH-RSA-AES256-SHA", "AES256-SHA",
  "ECDHE-ECDSA-DES-CBC3-SHA", "ECDHE-RSA-DES-CBC3-SHA", "EDH-RSA-DES-CBC3-SHA",
  "EDH-DSS-DES-CBC3-SHA", "ECDH-ECDSA-DES-CBC3-SHA", "ECDH-RSA-DES-CBC3-SHA",
  "DES-CBC3-SHA", "ECDHE-ECDSA-AES128-SHA", "ECDHE-RSA-AES128-SHA",
  "DHE-RSA-AES128-SHA", "DHE-DSS-AES128-SHA", "ECDH-ECDSA-AES128-SHA",
  "ECDH-RSA-AES128-SHA", "AES128-SHA"]
```

- 2 Sélectionnez les chiffrements pris en charge et conformes aux exigences de sécurité de votre organisation.

Par exemple, pour autoriser uniquement `ECDHE-ECDSA-AES128-GCM-SHA256` & `ECDHE-ECDSA-AES256-GCM-SHA384`, examinez le fichier `/etc/rabbitmq/rabbitmq.config` et ajoutez la ligne suivante à `ssl` et `ssl_options`.

```
{ciphers, ["ECDHE-ECDSA-AES128-GCM-SHA256", "ECDHE-ECDSA-AES256-GCM-SHA384"]}
```

- 3 Redémarrez le serveur RabbitMQ à l'aide de la commande suivante.

```
service rabbitmq-server restart
```

Vérification de la sécurité des données au repos

Vérifiez la sécurité des utilisateurs et des comptes de base de données utilisés avec vRealize Automation.

Utilisateur Postgres

Le compte d'utilisateur Postgres Linux est lié au rôle de compte de superutilisateur de la base de données Postgres. Ce compte est verrouillé par défaut. Il s'agit de la configuration la plus sécurisée pour cet utilisateur, car il est accessible uniquement à partir du compte d'utilisateur racine. Ne déverrouillez pas ce compte d'utilisateur.

Rôles de compte d'utilisateur de base de données

Les rôles par défaut des comptes d'utilisateur Postgres ne doivent pas être utilisés en dehors des fonctionnalités de l'application. Pour prendre en charge l'examen d'une base de données qui n'est pas celle par défaut ou les activités de rapport, vous devez créer un compte supplémentaire et le protéger correctement par un mot de passe.

Dans la ligne de commande, exécutez le script suivant :

```
vcac-vami add-db-user newUsername newPassword
```

Cela ajoutera un nouvel utilisateur et un mot de passe fourni par l'utilisateur.

Note Ce script doit être exécuté sur la base de données Postgres principale si une configuration Postgres HA principale/secondaire a été définie.

Configurer l'authentification du client PostgreSQL

Assurez-vous que l'authentification d'approbation locale n'est pas configurée dans la base de données PostgreSQL du dispositif vRealize Automation. En effet, cette configuration permet à tout utilisateur local, y compris le superutilisateur de la base de données, de se connecter en tant qu'utilisateur PostgreSQL sans mot de passe.

Note Le compte de superutilisateur Postgres doit rester un compte d'approbation locale.

La méthode d'authentification md5 est recommandée, car elle envoie des mots de passe chiffrés.

Les paramètres de configuration de l'authentification du client résident dans le fichier / storage/db/pgdata/pg_hba.conf.

#	TYPE	DATABASE	USER	ADDRESS	METHOD
# "local" is for Unix domain socket connections only					
local	all		postgres		trust
# IPv4 local connections:					
#host	all		all	127.0.0.1/32	md5
hostssl	all		all	127.0.0.1/32	md5
# IPv6 local connections:					
#host	all		all	:::1/128	md5
hostssl	all		all	:::1/128	md5
# Allow remote connections for VCAC user.					
#host	vcac		vcac	0.0.0.0/0	md5
hostssl	vcac		vcac	0.0.0.0/0	md5
hostssl	vcac		vcac	:::0/0	md5
# Allow remote connections for VCAC replication user.					
#host	vcac		vcac_replication	0.0.0.0/0	md5
hostssl	vcac		vcac_replication	0.0.0.0/0	md5
hostssl	vcac		vcac_replication	:::0/0	md5
# Allow replication connections by a user with the replication privilege.					
#host	replication		vcac_replication	0.0.0.0/0	md5
hostssl	replication		vcac_replication	0.0.0.0/0	md5
hostssl	replication		vcac_replication	:::0/0	md5

Si vous modifiez le fichier `pg_hba.conf`, vous devez redémarrer le serveur Postgres en exécutant les commandes suivantes afin que les modifications soient appliquées.

```
# cd /opt/vmware/vpostgres/9.2/bin
# su postgres
# ./pg_ctl restart -D /storage/db/pgdata/ -m fast
```

Configurer les ressources d'application de vRealize Automation

Vérifiez les ressources d'application de vRealize Automation et limitez les autorisations de fichier.

Procédure

- 1 Exécutez la commande suivante pour vérifier que les fichiers incluant des bits SUID et GUID sont bien définis.

```
find / -path /proc -prune -o -type f -perm +6000 -ls
```

La liste suivante doit s'afficher.

```
2197357  24 -rwsr-xr-x  1 polkituser root      23176 Mar 31  2015 /usr/lib/PolicyKit/polkit-
set-default-helper
2197354  16 -rwxr-sr-x  1 root      polkituser  14856 Mar 31  2015 /usr/lib/PolicyKit/polkit-
read-auth-helper
2197353  12 -rwsr-x---  1 root      polkituser  10744 Mar 31  2015 /usr/lib/PolicyKit/polkit-
grant-helper-pam
2197352  20 -rwxr-sr-x  1 root      polkituser  19208 Mar 31  2015 /usr/lib/PolicyKit/polkit-
grant-helper
2197351  20 -rwxr-sr-x  1 root      polkituser  19008 Mar 31  2015 /usr/lib/PolicyKit/polkit-
explicit-grant-helper
2197356  24 -rwxr-sr-x  1 root      polkituser  23160 Mar 31  2015 /usr/lib/PolicyKit/polkit-
revoke-helper
2188203  460 -rws---x--x  1 root      root      465364 Apr 21 22:38 /usr/lib64/ssh/ssh-keysign
2138858  12 -rwxr-sr-x  1 root      tty       10680 May 10  2010 /usr/sbin/utempter
2142482  144 -rwsr-xr-x  1 root      root      142890 Sep 15  2015 /usr/bin/passwd
2142477  164 -rwsr-xr-x  1 root      shadow    161782 Sep 15  2015 /usr/bin/chage
2142467  156 -rwsr-xr-x  1 root      shadow    152850 Sep 15  2015 /usr/bin/chfn
1458298  364 -rwsr-xr-x  1 root      root      365787 Jul 22  2015 /usr/bin/sudo
2142481  64 -rwsr-xr-x  1 root      root      57776 Sep 15  2015 /usr/bin/newgrp
1458249  40 -rwsr-x---  1 root      trusted   40432 Mar 18  2015 /usr/bin/crontab
2142478  148 -rwsr-xr-x  1 root      shadow    146459 Sep 15  2015 /usr/bin/chsh
2142480  156 -rwsr-xr-x  1 root      shadow    152387 Sep 15  2015 /usr/bin/gpasswd
2142479  48 -rwsr-xr-x  1 root      shadow    46967 Sep 15  2015 /usr/bin/expiry
311484  48 -rwsr-x---  1 root      messagebus 47912 Sep 16  2014 /lib64/dbus-1/dbus-daemon-
launch-helper
876574  36 -rwsr-xr-x  1 root      shadow    35688 Apr 10  2014 /sbin/unix_chkpwd
876648  12 -rwsr-xr-x  1 root      shadow    10736 Dec 16  2011 /sbin/unix2_chkpwd
 49308  68 -rwsr-xr-x  1 root      root      63376 May 27  2015 /opt/likewise/bin/ksu
1130552  40 -rwsr-xr-x  1 root      root      40016 Apr 16  2015 /bin/su
1130511  40 -rwsr-xr-x  1 root      root      40048 Apr 15  2011 /bin/ping
1130600  100 -rwsr-xr-x  1 root      root      94808 Mar 11  2015 /bin/mount
1130601  72 -rwsr-xr-x  1 root      root      69240 Mar 11  2015 /bin/umount
1130512  36 -rwsr-xr-x  1 root      root      35792 Apr 15  2011 /bin/ping6  2012 /lib64/
dbus-1/dbus-daemon-launch-helper
```

- 2 Exécutez la commande suivante pour vérifier que tous les fichiers du dispositif virtuel ont un propriétaire.

```
find / -path /proc -prune -o -nouser -o -nogroup
```

- 3 Vérifiez les autorisations de tous les fichiers du dispositif virtuel pour vous assurer qu'aucun d'entre eux ne peut faire l'objet d'une écriture par tout le monde en exécutant la commande suivante.

```
find / -name "*.*)" -type f -perm -a+w | xargs ls -ldb
```

- 4 Exécutez la commande suivante pour vérifier que seul l'utilisateur vcac possède les fichiers appropriés.

```
find / -name "proc" -prune -o -user vcac -print | egrep -v -e "*/vcac/*" | egrep -v -e "*/vmware-vcac/*"
```

Si aucun résultat n'apparaît, tous les fichiers corrects appartiennent uniquement à l'utilisateur vcac.

- 5 Vérifiez que les fichiers suivants sont accessibles en écriture uniquement par l'utilisateur vcac.

```
/etc/vcac/vcac/security.properties
/etc/vcac/vcac/solution-users.properties
/etc/vcac/vcac/sso-admin.properties
/etc/vcac/vcac/vcac.keystore
/etc/vcac/vcac/vcac.properties
```

Vérifiez également les fichiers suivants et leurs sous-répertoires.

```
/var/log/vcac/*
/var/lib/vcac/*
/var/cache/vcac/*
```

- 6 Vérifiez que seul l'utilisateur vcac ou racine peut lire les fichiers corrects dans les répertoires et sous-répertoires suivants.

```
/etc/vcac/*
/var/log/vcac/*
/var/lib/vcac/*
/var/cache/vcac/*
```

- 7 Vérifiez que les fichiers corrects appartiennent uniquement à l'utilisateur racine ou vco, comme illustré dans les répertoires et sous-répertoires suivants.

```
/etc/vco/*
/var/log/vco/*
/var/lib/vco/*
```

`/var/cache/vco/*`

- 8 Vérifiez que les fichiers corrects sont accessibles en écriture uniquement par l'utilisateur racine ou vco, comme illustré dans les répertoires suivants et leurs sous-répertoires.

`/etc/vco/*`

`/var/log/vco/*`

`/var/lib/vco/*`

`/var/cache/vco/*`

- 9 Vérifiez que les fichiers corrects sont accessibles en lecture seule par l'utilisateur racine ou vco, comme illustré dans les répertoires et sous-répertoires suivants.

`/etc/vco/*`

`/var/log/vco/*`

`/var/lib/vco/*`

`/var/cache/vco/*`

Personnalisation de la configuration du proxy de la console

Vous pouvez personnaliser la configuration de la console distante de vRealize Automation afin de simplifier le dépannage et les méthodes d'organisation.

Lorsque vous installez, configurez ou maintenez vRealize Automation, vous pouvez modifier certains paramètres pour activer le dépannage et le débogage de votre installation. Répertoriez et vérifiez chacune des modifications effectuées pour vous assurer que les composants applicables sont correctement sécurisés en fonction de l'utilisation requise. Ne les appliquez pas dans un environnement de production si vous n'êtes pas certain que les modifications de configuration sont correctement sécurisées.

Personnaliser le délai d'expiration des tickets de VMware Remote Console

Vous pouvez personnaliser la période de validité des tickets de la console distante permettant d'établir des connexions VMware Remote Console.

Lorsqu'un utilisateur établit des connexions VMware Remote Console, le système crée et renvoie des informations d'identification à usage unique pour une connexion spécifique à une machine virtuelle. Vous pouvez définir le délai d'expiration du ticket sur un intervalle de temps spécifié en minutes.

Procédure

- 1 Ouvrez le fichier `/etc/vcac/security.properties` dans un éditeur de texte.

- 2 Ajoutez au fichier une ligne au format `consoleproxy.ticket.validitySec=30`.

Sur cette ligne, la valeur numérique indique le nombre de minutes au terme desquelles le ticket expirera.

- 3 Enregistrez le fichier et fermez-le.

- 4 Redémarrez le serveur vCAC à l'aide de la commande `/etc/init.d/vcac-server restart`.

Résultats

La valeur du délai d'expiration du ticket est réinitialisée sur la période spécifiée en minutes.

Personnaliser le port de serveur proxy de la console

Vous pouvez personnaliser le port sur lequel le proxy de console VMware Remote Console écoute les messages.

Procédure

- 1 Ouvrez le fichier `/etc/vcac/security.properties` dans un éditeur de texte.
- 2 Ajoutez au fichier une ligne au format `consoleproxy.service.port=8445`.
La valeur numérique indique le numéro de port du service proxy de la console, dans ce cas 8445.
- 3 Enregistrez le fichier et fermez-le.
- 4 Redémarrez le serveur vCAC à l'aide de la commande `/etc/init.d/vcac-server restart`.

Résultats

Le port du service proxy est remplacé par le numéro de port spécifié.

Configurer l'en-tête de réponse X-XSS-Protection

Ajoutez l'en-tête de réponse X XSS-Protection au fichier de configuration haproxy.

Procédure

- 1 Ouvrez le fichier `/etc/haproxy/conf.d/20-vcac.cfg` pour le modifier.
- 2 Ajoutez les lignes suivantes dans la section frontale :

```
rspdel X-XSS-Protection:\ 1;\ mode=block
rspadd X-XSS-Protection:\ 1;\ mode=block
```

- 3 Rechargez la configuration HAProxy à l'aide de la commande suivante.
`/etc/init.d/haproxy reload`

Configurer l'en-tête de réponse X-Content-Type-Options

Ajoutez l'en-tête de réponse X-Content-Type-Options à la configuration HAProxy.

Procédure

- 1 Ouvrez le fichier `/etc/haproxy/conf.d/20-vcac.cfg` pour le modifier.
- 2 Ajoutez les lignes suivantes dans la section frontale :

```
http-response set-header X-Content-Type-Options nosniff
```

- 3 Rechargez la configuration HAProxy à l'aide de la commande suivante.
`/etc/init.d/haproxy reload`

Configurer l'en-tête de réponse HTTP Strict Transport Security

Ajoutez l'en-tête de réponse HTTP Strict Transport Security (HSTS) à la configuration HAProxy.

Procédure

- 1 Ouvrez le fichier `/etc/haproxy/conf.d/20-vcac.cfg` pour le modifier.
- 2 Ajoutez les lignes suivantes dans la section frontale :

```
rspdel Strict-Transport-Security:\ max-age=31536000
rspadd Strict-Transport-Security:\ max-age=31536000
```

- 3 Rechargez la configuration HAProxy à l'aide de la commande suivante.
- ```
/etc/init.d/haproxy reload
```

**Configurer l'en-tête de réponse X-Frame-Options**

L'en-tête de réponse X-Frame-Options est dupliquée dans certains cas.

Il se peut que l'en-tête de réponse X-Frame-Options apparaisse deux fois, car le service vIDM ajoute cet en-tête au serveur principal ainsi qu'au service HAProxy. Pour empêcher cette duplication, vous pouvez appliquer une configuration appropriée.

**Procédure**

- 1 Ouvrez le fichier `/etc/haproxy/conf.d/20-vcac.cfg` pour le modifier.
  - 2 Recherchez la ligne suivante dans la section frontale :
- ```
rspadd X-Frame-Options:\ SAMEORIGIN
```
- 3 Ajoutez les lignes suivantes avant la ligne localisée à l'étape précédente :
- ```
rspdel X-Frame-Options:\ SAMEORIGIN
```
- 4 Rechargez la configuration HAProxy à l'aide de la commande suivante.
- ```
/etc/init.d/haproxy reload
```

Configuration des en-têtes de réponse de serveur

Pour garantir la sécurité, il est recommandé de configurer le système vRealize Automation pour limiter l'accès aux informations par des pirates.

Dans la mesure du possible, réduisez au strict minimum les informations partagées par votre système concernant les identités et la version. Les pirates et autres entités malveillantes pourraient utiliser ces informations pour cibler votre serveur Web ou une version spécifique.

Configurer l'en-tête de réponse du serveur Lighttpd

Il est recommandé de créer un en-tête de serveur vide pour le serveur lighttpd du dispositif vRealize Automation.

Procédure

- 1 Ouvrez le fichier `/opt/vmware/etc/lighttpd/lighttpd.conf` dans un éditeur de texte.
- 2 Ajoutez `server.tag = " "` au fichier.
- 3 Enregistrez les modifications et fermez le fichier.

- 4 Redémarrez le serveur lighttpd en exécutant la commande `# /opt/vmware/etc/init.d/vami-lighttpd restart`.

Configurer l'en-tête de réponse TCServeur pour le dispositif vRealize Automation

Il est recommandé de créer un en-tête de serveur vide personnalisé pour l'en-tête de réponse TCServeur utilisé avec le dispositif vRealize Automation afin de limiter la possibilité qu'un pirate obtienne des informations importantes.

Procédure

- 1 Ouvrez le fichier `/etc/vco/app-server/server.xml` dans un éditeur de texte.
- 2 Dans chaque élément `<Connector>`, ajoutez `server=""` ..
Par exemple : `<Connector protocol="HTTP/1.1" server="" />`
- 3 Enregistrez les modifications et fermez le fichier.
- 4 Redémarrez le serveur à l'aide de la commande suivante.

```
service vco-server restart
```

Configurer l'en-tête de réponse de serveur IIS (Internet Information Services)

Il est recommandé de créer un en-tête de serveur vide personnalisé pour le serveur IIS (Internet Information Services) utilisé avec le dispositif Identity Appliance pour limiter le risque que des pirates obtiennent des informations importantes.

Procédure

- 1 Ouvrez le fichier `C:\Windows\System32\inetsrv\urlscan\UrlScan.ini` dans un éditeur de texte.
- 2 Recherchez `RemoveServerHeader=0` et remplacez-le par `RemoveServerHeader=1`.
- 3 Enregistrez les modifications et fermez le fichier.
- 4 Redémarrez le serveur en exécutant la commande `iisreset`.

Étape suivante

Désactivez l'en-tête X-Powered By d'IIS en supprimant les en-têtes de réponse HTTP dans la liste de la console du Gestionnaire des services Internet.

- 1 Ouvrez la console du Gestionnaire des services Internet.
- 2 Ouvrez l'en-tête de réponse HTTP et supprimez-le de la liste.
- 3 Redémarrez le serveur en exécutant la commande `iisreset`.

Définir le délai d'expiration de session dispositif vRealize Automation

Configurez le paramètre de délai d'expiration de session sur dispositif vRealize Automation conformément à la stratégie de sécurité de votre entreprise.

Le délai d'expiration de session par défaut de dispositif vRealize Automation pour l'inactivité de l'utilisateur est de 30 minutes. Pour modifier cette valeur de délai d'expiration conformément à la stratégie de sécurité de votre organisation, modifiez le fichier `web.xml` sur la machine hôte dispositif vRealize Automation.

Procédure

- 1 Ouvrez le fichier `/usr/lib/vcac/server/webapps/vcac/WEB-INF/web.xml` dans un éditeur de texte.
- 2 Recherchez `session-config` et définissez la valeur de délai d'expiration de la session. Reportez-vous à l'exemple de code suivant.

```
<!-- 30 minutes session expiration time -->
<session-config>
  <session-timeout>30</session-timeout>
  <tracking-mode>COOKIE</tracking-mode>
  <cookie-config>
    <path>/</path>
  </cookie-config>
</session-config>
```

- 3 Redémarrez le serveur en exécutant la commande suivante :

```
service vcac-server restart
```

Gestion des logiciels non essentiels

Pour réduire les risques de sécurité, supprimez ou configurez les logiciels non essentiels de vos machines hôtes vRealize Automation.

Configurez tous les logiciels que vous ne supprimez pas conformément aux recommandations du fabricant et aux meilleures pratiques de sécurité, afin de minimiser les risques de failles de sécurité.

Sécuriser le gestionnaire de stockage de masse USB

Sécurisez le gestionnaire de stockage de masse USB pour empêcher son utilisation en tant que gestionnaire de périphériques USB sur les machines hôtes du dispositif virtuel VMware, car il pourrait être utilisé pour compromettre la sécurité de votre système.

Procédure

- 1 Ouvrez le fichier `/etc/modprobe.conf.local` dans un éditeur de texte.
- 2 Assurez-vous que la ligne `install usb-storage /bin/true` apparaît dans le fichier.
- 3 Enregistrez le fichier et fermez-le.

Sécuriser le gestionnaire de protocole Bluetooth

Sécurisez le gestionnaire de protocole Bluetooth sur les machines hôtes du dispositif virtuel pour empêcher les pirates potentiels de l'exploiter.

La liaison du protocole Bluetooth à la pile réseau n'est pas nécessaire et risque d'augmenter la surface d'attaque de l'hôte.

Procédure

- 1 Ouvrez le fichier `/etc/modprobe.conf.local` dans un éditeur de texte.
- 2 Assurez-vous que la ligne suivante apparaît dans ce fichier.

```
install bluetooth /bin/true
```

- 3 Enregistrez le fichier et fermez-le.

Sécuriser le protocole Stream Control Transmission (SCTP)

Empêchez le protocole Stream Control Transmission (SCTP) de se charger sur votre système par défaut, car il pourrait être utilisé par des pirates pour compromettre la sécurité de votre système.

Configurez votre système pour empêcher le module SCTP de se charger, sauf si cela est absolument nécessaire. Le protocole SCTP est un protocole de couche de transport normalisé par l'IETF qui est devenu obsolète. La liaison de ce protocole à la pile réseau augmente la surface d'attaque de l'hôte. Les processus locaux sans privilèges risquent d'entraîner le chargement dynamique du gestionnaire de protocole par le noyau, en ouvrant un socket à l'aide de ce protocole.

Procédure

- 1 Ouvrez le fichier `/etc/modprobe.conf.local` dans un éditeur de texte.
- 2 Assurez-vous que la ligne suivante apparaît dans ce fichier.

```
install sctp /bin/true
```

- 3 Enregistrez le fichier et fermez-le.

Sécuriser le protocole Datagram Congestion (DCCP)

Dans le cadre de la sécurisation renforcée du système, empêchez le protocole Datagram Congestion (DCCP) de se charger sur les machines hôtes du dispositif virtuel par défaut, car il pourrait être utilisé pour compromettre la sécurité de votre système.

Évitez de charger le module du protocole DCCP, sauf si cela est absolument nécessaire. Le protocole DCCP résulte d'une proposition de protocole de couche de transport qui n'est pas utilisée. La liaison de ce protocole à la pile réseau augmente la surface d'attaque de l'hôte. Les processus locaux sans privilèges risquent d'entraîner le chargement dynamique du gestionnaire de protocole par le noyau en utilisant le protocole pour ouvrir un socket.

Procédure

- 1 Ouvrez le fichier `/etc/modprobe.conf.local` dans un éditeur de texte.
- 2 Assurez-vous que les lignes DCCP apparaissent dans le fichier.

```
install dccp/bin/true
install dccp_ipv4/bin/true
install dccp_ipv6/bin/true
```

- 3 Enregistrez le fichier et fermez-le.

Sécuriser le pontage réseau

Empêchez le module de pontage réseau de se charger sur votre système par défaut, car ce module pourrait être utilisé pour compromettre la sécurité de votre système.

Configurez votre système pour empêcher le réseau de se charger, sauf si cela est absolument nécessaire. En effet, des pirates pourraient l'exploiter pour contourner le partitionnement du réseau et ses mesures de sécurité.

Procédure

- 1 Exécutez la commande suivante sur toutes les machines hôtes du dispositif virtuel VMware.

```
# rmmod bridge
```

- 2 Ouvrez le fichier `/etc/modprobe.conf.local` dans un éditeur de texte.

- 3 Assurez-vous que la ligne suivante apparaît dans ce fichier.

```
install bridge /bin/false
```

- 4 Enregistrez le fichier et fermez-le.

Sécuriser le protocole Reliable Datagram Sockets (RDS)

Dans le cadre de la sécurisation renforcée du système, empêchez le protocole Reliable Datagram Sockets (RDS) de se charger sur les machines hôtes du dispositif virtuel par défaut, car il pourrait être utilisé pour compromettre la sécurité de votre système.

La liaison du protocole RDS à la pile réseau augmente la surface d'attaque de l'hôte. Les processus locaux sans privilèges risquent d'entraîner le chargement dynamique du gestionnaire de protocole par le système en utilisant le protocole pour ouvrir un socket.

Procédure

- 1 Ouvrez le fichier `/etc/modprobe.conf.local` dans un éditeur de texte.

- 2 Assurez-vous que la ligne `install rds /bin/true` apparaît dans ce fichier.

- 3 Enregistrez le fichier et fermez-le.

Sécuriser le protocole Transparent Inter-Process Communication (TIPC)

Dans le cadre de la sécurisation renforcée du système, empêchez le protocole Transparent Inter-Process Communication (TIPC) de se charger sur les machines hôtes du dispositif virtuel par défaut, car il pourrait être utilisé pour compromettre la sécurité de votre système.

La liaison du protocole TIPC à la pile réseau augmente la surface d'attaque de l'hôte. Les processus locaux sans privilèges risquent d'entraîner le chargement dynamique du gestionnaire de protocole par le noyau en utilisant le protocole pour ouvrir un socket.

Procédure

- 1 Ouvrez le fichier `/etc/modprobe.conf.local` dans un éditeur de texte.

- 2 Assurez-vous que la ligne `install tipc /bin/true` apparaît dans ce fichier.

- 3 Enregistrez le fichier et fermez-le.

Sécuriser le protocole Internetwork Packet Exchange (IPX)

Empêchez le protocole IPX (Internetwork Packet Exchange) de se charger sur votre système par défaut, car il pourrait être utilisé par des pirates pour compromettre la sécurité de votre système.

Évitez de charger le module du protocole IPX, sauf si cela est absolument nécessaire. Le protocole IPX est un protocole de couche réseau obsolète. La liaison de ce protocole à la pile réseau augmente la surface d'attaque de l'hôte. Les processus locaux sans privilèges risquent d'entraîner le chargement dynamique du gestionnaire de protocole par le système en utilisant le protocole pour ouvrir un socket.

Procédure

- 1 Ouvrez le fichier `/etc/modprobe.conf.local` dans un éditeur de texte.
- 2 Assurez-vous que la ligne suivante apparaît dans ce fichier.

```
install ipx /bin/true
```

- 3 Enregistrez le fichier et fermez-le.

Sécuriser le protocole Appletalk

Empêchez le protocole Appletalk de se charger sur votre système par défaut, car il pourrait être utilisé par des pirates pour compromettre la sécurité de votre système.

Évitez de charger le module du protocole Appletalk, sauf si cela est absolument nécessaire. La liaison de ce protocole à la pile réseau augmente la surface d'attaque de l'hôte. Les processus locaux sans privilèges risquent d'entraîner le chargement dynamique du gestionnaire de protocole par le système en utilisant le protocole pour ouvrir un socket.

Procédure

- 1 Ouvrez le fichier `/etc/modprobe.conf.local` dans un éditeur de texte.
- 2 Assurez-vous que la ligne suivante apparaît dans ce fichier.

```
install appletalk /bin/true
```

- 3 Enregistrez le fichier et fermez-le.

Sécuriser le protocole DECnet

Empêchez le protocole DECnet de se charger sur votre système par défaut, car il pourrait être utilisé par des pirates pour compromettre la sécurité de votre système.

Évitez de charger le module du protocole DECnet, sauf si cela est absolument nécessaire. La liaison de ce protocole à la pile réseau augmente la surface d'attaque de l'hôte. Les processus locaux sans privilèges risquent d'entraîner le chargement dynamique du gestionnaire de protocole par le système en utilisant le protocole pour ouvrir un socket.

Procédure

- 1 Ouvrez le fichier de protocole DECnet `/etc/modprobe.conf.local` dans un éditeur de texte.
- 2 Assurez-vous que la ligne suivante apparaît dans ce fichier.

```
install decnet /bin/true
```

3 Enregistrez le fichier et fermez-le.

Sécuriser le module Firewire

Empêchez le module Firewire de se charger sur votre système par défaut. car il pourrait être utilisé par des pirates pour compromettre la sécurité de votre système.

Évitez de charger le module Firewire, sauf si cela est absolument nécessaire.

Procédure

1 Ouvrez le fichier `/etc/modprobe.conf.local` dans un éditeur de texte.

2 Assurez-vous que la ligne suivante apparaît dans ce fichier.

```
install ieee1394 /bin/true
```

3 Enregistrez le fichier et fermez-le.

Sécurisation du composant IaaS (Infrastructure en tant que service)

Lorsque vous renforcez la sécurité de votre système, sécurisez le composant IaaS (Infrastructure en tant que service) vRealize Automation et sa machine hôte pour les protéger contre les pirates.

Vous devez configurer le paramètre de sécurité du composant IaaS (Infrastructure en tant que service) vRealize Automation et de l'hôte sur lequel il réside. Vous devez définir ou vérifier la configuration des autres applications et composants connexes. Dans certains cas, vous pouvez vérifier les paramètres existants, dans d'autres vous devez modifier ou ajouter des paramètres pour une configuration appropriée.

Configuration de NTP

Pour garantir la sécurité, il est recommandé d'utiliser des serveurs de temps autorisés plutôt que la synchronisation date/heure des hôtes dans un environnement de production vRealize Automation.

Dans un environnement de production, désactivez la synchronisation date/heure des hôtes et utilisez des serveurs de temps autorisés pour assurer le suivi précis des actions des utilisateurs et identifier d'éventuelles attaques malveillantes et intrusions au moyen d'un audit et d'une journalisation détaillés.

Configuration de TLS pour les données en transit d'IaaS (Infrastructure en tant que service)

Assurez-vous que votre déploiement vRealize Automation utilise des protocoles TLS forts afin de sécuriser les canaux de transmission pour les composants IaaS (Infrastructure en tant que service).

Les protocoles de chiffrement SSL (Secure Sockets Layer) et TLS (Transport Layer Security), ce dernier ayant été plus récemment développé, garantissent la sécurité du système lors des communications réseau entre différents composants système. La norme du protocole SSL étant plus ancienne, un grand nombre de ses implémentations ne fournissent plus une sécurité adéquate contre les attaques potentielles. De graves faiblesses ont été identifiées avec des protocoles SSL antérieurs, notamment SSLv2 et SSLv3. Ces protocoles ne sont plus considérés comme sécurisés.

Selon les stratégies de sécurité de votre organisation, vous pouvez également désactiver TLS 1.0.

Note Lors de l'arrêt de TLS sur l'équilibrage de charge, désactivez également les protocoles faibles tels que SSLv2, SSLv3, ainsi que TLS 1.0 et 1.1 si nécessaire.

Activer les protocoles TLS 1.1 et 1.2 pour IaaS

Activez et appliquez l'utilisation des protocoles TLS 1.1 et 1.2 sur toutes les machines virtuelles qui hébergent des composants IaaS.

Procédure

1 Cliquez sur **Démarrer**, puis sur **Exécuter**.

2 Entrez Regedit, puis cliquez sur **OK**.

3 Localisez et ouvrez la sous-clé de registre suivante.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SChannel\Protocols

4 Vérifiez les éléments suivants et créez des entrées si nécessaire.

- S'il n'y a pas de sous-clé nommée TLS 1.1 sous Protocols, créez-en une.
- S'il n'y a pas de sous-clé nommée Client sous TLS 1.1, créez-en une.
- S'il n'y a pas de clé nommée DisabledByDefault dans la sous-clé Client, créez-en une de type DWORD.
- Cliquez avec le bouton droit sur DisabledByDefault, sélectionnez Modifier et définissez sa valeur sur 0.
- S'il n'y a pas de clé nommée Enabled dans la sous-clé Client, créez-en une de type DWORD.
- Cliquez avec le bouton droit sur Enabled, sélectionnez Modifier et définissez sa valeur sur 1.
- S'il n'y a pas de sous-clé nommée Server sous TLS 1.1, créez-en une.
- S'il n'y a pas de clé nommée DisabledByDefault dans la sous-clé Server, créez-en une de type DWORD.
- Cliquez avec le bouton droit sur DisabledByDefault, sélectionnez Modifier et définissez sa valeur sur 0.
- S'il n'y a pas de clé nommée Enabled dans la sous-clé de Server, créez-en une de type DWORD.
- Cliquez avec le bouton droit sur Enabled, sélectionnez Modifier et définissez sa valeur sur 1.

5 Répétez l'étape précédente pour le protocole TLS 1.2.

Note Pour appliquer l'utilisation de TLS 1.1 et 1.2, des paramètres supplémentaires sont requis, comme décrit dans les étapes suivantes.

6 Localisez et ouvrez la sous-clé de registre suivante.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319

7 Vérifiez les éléments suivants et créez des entrées si nécessaire.

- S'il n'y a pas d'entrée DWORD nommée SchUseStrongCrypto, créez-la et définissez sa valeur sur 1.
- S'il n'y a pas d'entrée DWORD nommée SystemDefaultTlsVersions, créez-la et définissez sa valeur sur 1.

8 Localisez et ouvrez la sous-clé de registre suivante.

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v4.0.30319

9 Vérifiez les éléments suivants et créez des entrées si nécessaire.

- S'il n'y a pas d'entrée DWORD nommée SchUseStrongCrypto, créez-la et définissez sa valeur sur 1.
- S'il n'y a pas d'entrée DWORD nommée SystemDefaultTlsVersions, créez-la et définissez sa valeur sur 1.

Désactiver SSL 3.0 et TLS 1.0 pour IaaS

Désactivez SSL 3.0 et le protocole TLS 1.0 obsolète pour les composants IaaS.

Procédure

1 Cliquez sur **Démarrer**, puis sur **Exécuter**.

2 Entrez Regedit, puis cliquez sur **OK**.

3 Localisez et ouvrez la sous-clé de registre suivante.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols

4 Vérifiez les éléments suivants et créez des entrées si nécessaire.

- S'il n'y a pas de sous-clé nommée SSL 3.0 sous Protocols, créez-en une.
- S'il n'y a pas de sous-clé nommée Client sous SSL 3.0, créez-en une.
- S'il n'y a pas de clé nommée DisabledByDefault dans la sous-clé Client, créez-en une de type DWORD.
- Cliquez avec le bouton droit sur DisabledByDefault, sélectionnez Modifier et définissez sa valeur sur 1.
- Cliquez avec le bouton droit sur Enabled, sélectionnez Modifier et définissez sa valeur sur 0.
- S'il n'y a pas de sous-clé nommée Server sous SSL 3.0, créez-en une.
- S'il n'y a pas de clé nommée DisabledByDefault dans la sous-clé Server, créez-en une de type DWORD.

- Cliquez avec le bouton droit sur DisabledByDefault, sélectionnez Modifier et définissez sa valeur sur 1.
- S'il n'y a pas de clé nommée Enabled dans Server, créez-en une de type DWORD.
- Cliquez avec le bouton droit sur Enabled, sélectionnez Modifier et définissez sa valeur sur 0.

5 Répétez les étapes précédentes pour le protocole TLS 1.0.

Désactiver TLS 1.0 pour IaaS

Afin de garantir une sécurité maximale, configurez le service IaaS pour utiliser le pooling et désactivez TLS 1.0.

Pour plus d'informations, reportez-vous à l'article <https://support.microsoft.com/en-us/kb/245030> dans la Base de connaissances de Microsoft.

Procédure

1 Configurez le service IaaS pour utiliser le pooling au lieu de sockets Web.

- a Mettez à jour le fichier de configuration de Manager Service C:\Program Files (x86)\VMware\VCAC\Server\ManagerService.exe.config en ajoutant les valeurs suivantes dans la section <appSettings>.

```
<add key="Extensibility.Client.RetrievalMethod" value="Polling"/>
<add key="Extensibility.Client.PollingInterval" value="2000"/>
<add key="Extensibility.Client.PollingMaxEvents" value="128"/>
```

- b Redémarrez Manager Service (service VMware vCloud Automation Center).

2 Assurez-vous que TLS 1.0 est désactivé sur le serveur IaaS.

- a Exécutez l'éditeur de Registre en tant qu'administrateur.
- b Dans la fenêtre du Registre, accédez à HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\
- c Cliquez avec le bouton droit sur Protocoles et sélectionnez **Nouvelle > Clé**, puis entrez **TLS 1.0**.
- d Dans l'arborescence de navigation, cliquez avec le bouton droit sur la clé TLS 1.0 que vous venez de créer. Dans le menu contextuel, sélectionnez **Nouvelle > Clé** et entrez **Client**.
- e Dans l'arborescence de navigation, cliquez avec le bouton droit sur la clé TLS 1.0 que vous venez de créer. Dans le menu contextuel, sélectionnez **Nouvelle > Clé** et entrez **Server**.
- f Dans l'arborescence de navigation, dans la section TLS 1.0, cliquez avec le bouton droit sur **Client**, puis cliquez sur **Nouvelle > Valeur DWORD 32 bits** et entrez **DisabledByDefault**.

- g Dans l'arborescence de navigation, dans la section TLS 1.0, sélectionnez **Client**. Dans le volet de droite, double-cliquez sur **DisabledByDefault** (valeur DWORD) et entrez **1**.
- h Dans l'arborescence de navigation, dans la section TLS 1.0, cliquez avec le bouton droit sur **Serveur** et sélectionnez **Nouvelle > Valeur DWORD 32 bits** et entrez **Enabled**.
- i Dans l'arborescence de navigation, dans la section TLS 1.0, sélectionnez **Serveur**. Dans le volet de droite, double-cliquez sur **Activé** (valeur DWORD) et saisissez **0**.
- j Redémarrez le serveur Windows.

Configuration des suites de chiffrement TLS

Pour obtenir une sécurité maximale, vous devez configurer les composants vRealize Automation pour utiliser des chiffrements forts. Le chiffrement négocié entre le serveur et le navigateur détermine la force du chiffrement utilisé dans une session TLS. Pour vous assurer que seuls des chiffrements forts sont sélectionnés, désactivez les chiffrements faibles dans les composants vRealize Automation. Configurez le serveur pour prendre en charge uniquement les chiffrements forts et pour utiliser des clés suffisamment grandes. En outre, configurez tous les chiffrements dans l'ordre approprié.

Suites de chiffrement non acceptables

Désactivez les suites de chiffrement qui ne proposent pas d'authentification telles que les suites de chiffrement NULL, aNULL ou eNULL. Désactivez également l'échange de clés anonyme Diffie-Hellman (ADH), les chiffrements de niveau exportation (EXP, chiffrements contenant des algorithmes DES), les tailles de clé inférieures à 128 bits pour le chiffrement du trafic de la charge utile, l'utilisation de la fonction MD5 comme mécanisme de hachage pour le trafic de charge utile, les suites de chiffrement IDEA et les suites de chiffrement RC4. Assurez-vous également que les suites de chiffrement utilisant l'échange de clés Diffie-Hellman (DHE) sont désactivées.

Pour plus d'informations sur la désactivation des chiffrements de clés statiques dans vRealize Automation, reportez-vous à [l'article 71094 de la base de connaissances](#).

Vérification de la sécurité du serveur hôte

Une bonne pratique de sécurité consiste à vérifier la configuration de la sécurité des machines de votre serveur hôte IaaS (Infrastructure en tant que service).

Microsoft fournit plusieurs outils de vérification de la sécurité sur les machines du serveur hôte. Contactez votre fournisseur Microsoft pour obtenir des conseils sur l'utilisation la plus appropriée de ces outils.

Vérifier la sécurité de la ligne de base du serveur hôte

Exécutez Microsoft Baseline Security Analyzer (MBSA) pour vérifier rapidement que votre serveur dispose des dernières mises à jour ou des correctifs les plus récents. Vous pouvez utiliser MBSA pour installer des correctifs de sécurité manquants de Microsoft, afin de maintenir votre serveur à jour conformément aux recommandations de sécurité de Microsoft.

Téléchargez la dernière version de l'outil MBSA sur le site Web de Microsoft.

Vérifier la configuration de sécurité du serveur hôte

Utilisez l'Assistant Configuration de la sécurité de Windows et le kit de ressources Gestionnaire de conformité de sécurité Microsoft pour vérifier que le serveur hôte est configuré de manière sécurisée.

Exécutez l'Assistant Configuration de la sécurité de Windows à partir des outils d'administration de votre serveur Windows. Cet outil peut identifier les rôles de votre serveur et les fonctionnalités installées, notamment la mise en réseau, les pare-feu Windows et les paramètres de Registre. Comparez le rapport avec les derniers conseils en matière de sécurisation renforcée du Gestionnaire de conformité de sécurité Microsoft correspondant à votre serveur Windows. Selon les résultats, vous pouvez ajuster précisément les paramètres de sécurité pour chaque fonctionnalité, tels que les services réseau, les paramètres de compte et les pare-feu Windows, et appliquer les paramètres à votre serveur.

Pour plus d'informations sur l'Assistant Configuration de la sécurité de Windows, consultez le site Web Microsoft Technet.

Protection des ressources d'application

Pour garantir la sécurité, il est recommandé de vérifier que tous les fichiers laaS (Infrastructure en tant que service) pertinents disposent d'autorisations appropriées.

Vérifiez les fichiers laaS (Infrastructure en tant que service) par rapport à votre installation laaS. Dans la plupart des cas, les sous-dossiers et fichiers de chaque dossier doivent avoir les mêmes paramètres que le dossier.

Répertoire ou fichier	Groupe ou utilisateurs	Contrôle total	Modifier	Lire et exécuter	Lecture	Écriture
VMware\VCAC\Agents \<agent_name> \logs	SYSTÈME	X	X	X	X	X
	administrateur	X	X	X	X	X
	Administrateurs	X	X	X	X	X
VMware\VCAC\Agents\ <agent_name> \temp	SYSTÈME	X	X	X	X	X
	administrateur	X	X	X	X	X
	Administrateurs	X	X	X	X	X
VMware\VCAC\Agents\	SYSTÈME	X	X	X	X	X
	Administrateurs	X	X	X	X	X
	Utilisateurs			X	X	
VMware\VCAC\Distributed Execution Manager\	SYSTÈME	X	X	X	X	X
	Administrateurs	X	X	X	X	X
	Utilisateurs			X	X	

Répertoire ou fichier	Groupe ou utilisateurs	Contrôle total	Modifier	Lire et exécuter	Lecture	Écriture
VMware\VCAC\Distributed Execution Manager\DEM\Logs	SYSTÈME	X	X	X	X	X
	administrateur	X	X	X	X	X
	Administrateurs	X	X	X	X	X
VMware\VCAC\Distributed Execution Manager\DEO\Logs	SYSTÈME	X	X	X	X	X
	administrateur	X	X	X	X	X
	Administrateurs	X	X	X	X	X
VMware\VCAC\Management Agent\	SYSTÈME	X	X	X	X	X
	Administrateurs	X	X	X	X	X
	Utilisateurs			X	X	
VMware\VCAC\Server\	SYSTÈME	X	X	X	X	X
	Administrateurs	X	X	X	X	X
	Utilisateurs			X	X	
VMware\VCAC\Web API	SYSTÈME	X	X	X	X	X
	Administrateurs	X	X	X	X	X
	Utilisateurs			X	X	

Sécuriser la machine hôte IaaS (Infrastructure en tant que service)

Pour garantir la sécurité, il est recommandé de vérifier les paramètres de base sur votre machine hôte IaaS (Infrastructure en tant que service) pour vous assurer qu'elle est conforme aux directives de sécurité.

Sécurisez les comptes, applications, ports et services sur la machine hôte IaaS.

Vérifier les paramètres de compte d'utilisateur de serveur

Vérifiez qu'il n'existe pas de paramètres et de comptes d'utilisateur local et de domaine inutiles. Tout compte d'utilisateur non associé aux fonctions d'application doit être réservé à l'administration, à la maintenance et au dépannage. Limitez l'accès distant à partir de comptes d'utilisateurs de domaine au minimum requis pour maintenir le serveur. Réalisez des contrôles et audits stricts de ces comptes.

Supprimez les applications inutiles

Supprimez toutes les applications inutiles des serveurs hôtes. Les applications inutiles augmentent le risque d'exposition en raison de leurs vulnérabilités inconnues ou non corrigées.

Désactiver les ports et services inutiles

Passez en revue la liste des ports ouverts du pare-feu du serveur hôte. Bloquez tous les ports qui ne sont pas requis pour le composant IaaS ou le fonctionnement critique du système. Consultez [Configuration des ports et des protocoles](#). Vérifiez les services en cours d'exécution sur votre serveur hôte et désactivez ceux qui ne sont pas requis.

Configuration de la sécurité réseau des hôtes

Pour assurer une protection maximale contre les menaces de sécurité connues, configurez les paramètres d'interface et de communication réseau sur toutes les machines hôtes VMware.

Dans le cadre d'un plan de sécurité complet, configurez les paramètres de sécurité d'interface réseau pour les dispositifs virtuels VMware et les composants IaaS (Infrastructure en tant que service) conformément aux directives de sécurité établies.

Configuration des paramètres réseau pour les dispositifs VMware

Pour vous assurer que les machines hôtes du dispositif virtuel VMware prennent uniquement en charge des communications sécurisées et importantes, vérifiez et modifiez leurs paramètres de communication réseau.

Examinez la configuration du protocole IP du réseau de vos machines hôtes VMware et configurez les paramètres réseau conformément aux directives de sécurité. Désactivez tous les protocoles de communication non essentiels.

Empêcher le contrôle par l'utilisateur des interfaces réseau

Pour garantir la sécurité, il est recommandé d'accorder aux utilisateurs uniquement les privilèges système indispensables pour effectuer leurs tâches sur les machines hôtes du dispositif VMware.

Le fait d'autoriser des comptes d'utilisateur disposant de privilèges à manipuler des interfaces réseau risque de créer des mécanismes de contournement de la sécurité réseau ou un déni de service. Limitez les possibilités de modification des paramètres d'interface réseau aux utilisateurs disposant de privilèges.

Procédure

- 1 Exécutez la commande suivante sur chaque machine hôte du dispositif VMware.

```
# grep -i '^USERCONTROL=' /etc/sysconfig/network/ifcfg*
```

- 2 Assurez-vous que chaque interface est définie sur NO.

Définir la taille de la file d'attente du backlog TCP

Pour fournir un niveau de défense contre les attaques malveillantes, configurez une taille de file d'attente de backlog TCP par défaut sur les machines hôtes du dispositif VMware.

Définissez les tailles des files d'attente de backlog TCP sur une taille par défaut appropriée pour une meilleure prévention contre les attaques de service ou de refus du TCP. La valeur par défaut recommandée du paramètre est de 1280.

Procédure

- 1 Exécutez la commande suivante sur chaque machine hôte du dispositif VMware.

```
# cat /proc/sys/net/ipv4/tcp_max_syn_backlog
```

- 2 Ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.
- 3 Définissez la taille de la file d'attente du backlog TCP par défaut en ajoutant l'entrée suivante au fichier.

```
net.ipv4.tcp_max_syn_backlog=1280
```

- 4 Enregistrez les modifications et fermez le fichier.

Refuser les demandes d'écho ICMPv4 d'adresse de diffusion

Pour garantir la sécurité, il est recommandé de vérifier que les machines hôtes du dispositif VMware ignorent les demandes d'écho d'adresse de diffusion ICMP.

Les réponses pour diffuser les demandes d'écho ICMP (Internet Control Message Protocol) fournissent un vecteur d'attaque d'amplification et peuvent faciliter le mappage réseau par des agents malveillants. La configuration des machines hôtes de dispositif pour ignorer les demandes d'écho ICMPv4 fournit une protection contre de telles attaques.

Procédure

- 1 Exécutez la commande `# cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts` sur les machines hôtes du dispositif virtuel VMware pour confirmer qu'elles refusent des demandes d'écho d'adresse de diffusion IPv4.

Si les machines hôtes sont configurées pour refuser les redirections IPv4, cette commande renvoie la valeur 0 pour `/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts`.

- 2 Pour configurer une machine hôte de dispositif virtuel pour refuser les demandes d'écho d'adresse de diffusion ICMPv4, ouvrez le fichier `/etc/sysctl.conf` sur les machines hôtes Windows dans un éditeur de texte.
- 3 Localisez l'entrée contenant `net.ipv4.icmp_echo_ignore_broadcasts=0`. Si la valeur de cette entrée n'est pas définie sur zéro ou si l'entrée n'existe pas, ajoutez-la ou mettez à jour l'entrée existante.
- 4 Enregistrez les modifications et fermez le fichier.

Désactiver le protocole ARP du proxy IPv4

Assurez-vous que le protocole ARP du proxy IPv4 est désactivé, s'il n'est pas requis sur les machines hôtes du dispositif VMware, afin d'empêcher le partage non autorisé d'informations.

Le protocole ARP du proxy IPv4 permet à un système d'envoyer des réponses aux demandes ARP sur une interface pour le compte d'hôtes connectés à une autre interface. Désactivez cette fonctionnalité si elle ne sert pas à empêcher la fuite d'informations d'adressage entre les segments réseau attachés.

Procédure

- 1 Exécutez la commande `# grep [01] /proc/sys/net/ipv4/conf/*/proxy_arp | egrep "default|all"` sur les machines hôtes du dispositif virtuel VMware pour vérifier que le protocole ARP du proxy IPv4 est désactivé.

Si le protocole ARP du proxy IPv6 est désactivé sur les machines hôtes, cette commande renvoie des valeurs 0.

```
/proc/sys/net/ipv4/conf/all/proxy_arp:0
/proc/sys/net/ipv4/conf/default/proxy_arp:0
```

Si les machines hôtes sont correctement configurées, aucune autre action n'est nécessaire.

- 2 Si vous devez configurer le protocole ARP du proxy IPv6 sur les machines hôtes, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.
- 3 Recherchez les entrées suivantes.

```
net.ipv4.conf.default.proxy_arp=0
net.ipv4.conf.all.proxy_arp=0
```

Si les entrées n'existent pas ou si leurs valeurs ne sont pas définies sur zéro, ajoutez les entrées ou mettez à jour les entrées existantes.

- 4 Enregistrez les modifications et fermez le fichier.

Refuser les messages de redirection ICMP IPv4

Pour garantir la sécurité, il est recommandé de vérifier que les machines hôtes du dispositif virtuel VMware refusent les messages de redirection ICMP IPv4.

Les routeurs utilisent des messages de redirection ICMP pour informer les hôtes qu'une route plus directe existe pour une destination. Un message de redirection ICMP malveillant peut faciliter une attaque de l'intercepteur. Ces messages modifient la table de routage de l'hôte et ne sont pas authentifiés. Assurez-vous que votre système est configuré pour les ignorer s'ils ne sont pas nécessaires.

Procédure

- 1 Exécutez la commande `# grep [01] /proc/sys/net/ipv4/conf/*/accept_redirects | egrep "default|all"` sur les machines hôtes de dispositif VMware afin de confirmer le refus des messages de redirection IPv4.

Si les machines hôtes sont configurées pour refuser les redirections IPv4, cette commande renvoie ce qui suit :

```
/proc/sys/net/ipv4/conf/all/accept_reidrects:0
/proc/sys/net/ipv4/conf/default/accept_redirects:0
```

- 2 Si vous devez configurer une machine hôte de dispositif virtuel pour refuser les messages de redirection IPv4, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.

3 Vérifiez les valeurs des lignes qui commencent par `net.ipv4.conf`.

Si les valeurs des entrées suivantes ne sont pas définies sur zéro ou si les entrées n'existent pas, ajoutez-les au fichier ou mettez à jour les entrées existantes.

```
net.ipv4.conf.all.accept_redirects=0
net.ipv4.conf.default.accept_redirects=0
```

4 Enregistrez les modifications et fermez le fichier.

Refuser les messages de redirection ICMP IPv6

Pour garantir la sécurité, il est recommandé de vérifier que les machines hôtes du dispositif virtuel VMware refusent les messages de redirection ICMP IPv6.

Les routeurs utilisent des messages de redirection ICMP pour informer les hôtes qu'une route plus directe existe pour une destination. Un message de redirection ICMP malveillant peut faciliter une attaque de l'intercepteur. Ces messages modifient la table de routage de l'hôte et ne sont pas authentifiés. Assurez-vous que votre système est configuré pour les ignorer s'ils ne sont pas nécessaires.

Procédure

1 Exécutez la commande `# grep [01] /proc/sys/net/ipv6/conf/*/accept_redirects | egrep "default|all"` sur les machines hôtes du dispositif virtuel VMware pour confirmer le refus des messages de redirection IPv6.

Si les machines hôtes sont configurées pour refuser les redirections IPv6, cette commande renvoie ce qui suit :

```
/proc/sys/net/ipv6/conf/all/accept_redirects:0
/proc/sys/net/ipv6/conf/default/accept_redirects:0
```

2 Pour configurer une machine hôte de dispositif virtuel pour refuser les messages de redirection IPv4, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.

3 Vérifiez les valeurs des lignes qui commencent par `net.ipv6.conf`.

Si les valeurs des entrées suivantes ne sont pas définies sur zéro ou si elles n'existent pas, ajoutez-les au fichier ou mettez à jour les entrées existantes.

```
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```

4 Enregistrez les modifications et fermez le fichier.

Journaliser des paquets martiens IPv4

Pour garantir la sécurité, il est recommandé de vérifier que les machines hôtes du dispositif virtuel VMware journalisent les paquets martiens IPv4.

Les paquets martiens contiennent des adresses identifiées comme non valides par le système. Configurez les machines hôtes pour journaliser ces messages, de façon à identifier les configurations incorrectes ou les attaques en cours.

Procédure

- 1 Exécutez la commande `# grep [01] /proc/sys/net/ipv4/conf/*/log_martians | grep "default|all"` sur les machines hôtes du dispositif VMware pour vérifier la journalisation des paquets martiens IPv4.

Si les machines virtuelles sont configurées pour journaliser les paquets martiens, elles renvoient ce qui suit :

```
/proc/sys/net/ipv4/conf/all/log_martians:1
/proc/sys/net/ipv4/conf/default/log_martians:1
```

Si les machines hôtes sont correctement configurées, aucune autre action n'est nécessaire.

- 2 Si vous devez configurer des machines virtuelles pour journaliser des paquets martiens IPv4, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.
- 3 Vérifiez les valeurs des lignes qui commencent par `net.ipv4.conf`.

Si la valeur des entrées suivantes n'est pas définie sur 1 ou si ces entrées n'existent pas, ajoutez-les au fichier ou mettez à jour les entrées existantes.

```
net.ipv4.conf.all.log_martians=1
net.ipv4.conf.default.log_martians=1
```

- 4 Enregistrez les modifications et fermez le fichier.

Utiliser le filtrage de chemin inverse IPv4

Pour garantir la sécurité, il est recommandé de vérifier que les machines hôtes de VMware utilisent le filtrage de chemin inverse IPv4.

Le filtrage de chemin inverse constitue une protection contre l'usurpation des adresses source en provoquant le rejet des paquets dont les adresses source n'ont aucune route ou dont la route ne pointe pas vers l'interface d'origine. Configurez vos machines hôtes pour utiliser le filtrage de chemin inverse autant que possible. Dans certains cas, selon le rôle système, le filtrage de chemin inverse peut entraîner le rejet d'un trafic légitime. Si vous rencontrez de tels problèmes, vous devrez éventuellement utiliser un mode plus permissif ou désactiver complètement le filtrage de chemin inverse.

Procédure

- 1 Exécutez la commande `# grep [01] /proc/sys/net/ipv4/conf/*/rp_filter|egrep "default|all"` sur les machines hôtes du dispositif virtuel VMware pour vérifier qu'elles utilisent le filtrage de chemin inverse IPv4.

Si les machines virtuelles utilisent le filtrage de chemin inverse IPv4, cette commande renvoie ce qui suit :

```
/proc/sys/net/ipv4/conf/all/rp_filter:1
/proc/sys/net/ipv4/conf/default/rp_filter:1
```

Si vos machines virtuelles sont correctement configurées, aucune autre action n'est requise.

- 2 Si vous devez configurer le filtrage de chemin inverse IPv4 sur des machines hôtes, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.
- 3 Vérifiez les valeurs des lignes qui commencent par `net.ipv4.conf`.

Si les valeurs des entrées suivantes ne sont pas définies sur 1 ou si elles n'existent pas, ajoutez-les au fichier ou mettez à jour les entrées existantes.

```
net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.default.rp_filter=1
```

- 4 Enregistrez les modifications et fermez le fichier.

Refuser le transfert IPv4

Vérifiez que les machines hôtes du dispositif VMware refusent le transfert IPv4.

Si le système est configuré pour le transfert IP et n'est pas un routeur désigné, les pirates peuvent l'utiliser pour contourner la sécurité du réseau en fournissant un chemin de communication non filtré par les périphériques réseau. Configurez les machines hôtes du dispositif virtuel pour refuser le transfert IPv4 afin d'éliminer ce risque.

Procédure

- 1 Exécutez la commande `# cat /proc/sys/net/ipv4/ip_forward` sur les machines hôtes du dispositif VMware afin de confirmer qu'elles refusent les transferts IPv4.

Si les machines hôtes sont configurées pour refuser le transfert IPv4, cette commande renvoie la valeur 0 pour `/proc/sys/net/ipv4/ip_forward`. Si les machines virtuelles sont correctement configurées, aucune autre action n'est nécessaire.

- 2 Pour configurer une machine hôte de dispositif virtuel pour refuser le transfert IPv4, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.
- 3 Localisez l'entrée contenant `net.ipv4.ip_forward=0`. Si la valeur de cette entrée n'est pas définie sur zéro ou si l'entrée n'existe pas, ajoutez-la ou mettez à jour l'entrée existante.
- 4 Enregistrez les modifications et fermez le fichier.

Refuser le transfert IPv6

Pour garantir la sécurité, il est recommandé de vérifier que vos systèmes hôtes de dispositif VMware refusent le transfert IPv6.

Si le système est configuré pour le transfert IP et n'est pas un routeur désigné, les pirates peuvent l'utiliser pour contourner la sécurité du réseau en fournissant un chemin de communication non filtré par les périphériques réseau. Configurez les machines hôtes de dispositif virtuel pour refuser le transfert IPv6 afin d'éliminer ce risque.

Procédure

- 1 Exécutez la commande `# grep [01] /proc/sys/net/ipv6/conf/*/forwarding | grep "default|all"` sur les machines hôtes du dispositif VMware pour vérifier qu'elles refusent le transfert IPv6.

Si les machines hôtes sont configurées pour refuser le transfert IPv6, cette commande renvoie ce qui suit :

```
/proc/sys/net/ipv6/conf/all/forwarding:0
/proc/sys/net/ipv6/conf/default/forwarding:0
```

Si les machines hôtes sont correctement configurées, aucune autre action n'est nécessaire.

- 2 Si vous devez configurer une machine hôte pour refuser le transfert IPv6, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.
- 3 Vérifiez les valeurs des lignes qui commencent par `net.ipv6.conf`.

Si les valeurs des entrées suivantes ne sont pas définies sur zéro ou si les entrées n'existent pas, ajoutez les entrées ou mettez à jour les entrées existantes en conséquence.

```
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```

- 4 Enregistrez les modifications et fermez le fichier.

Utiliser des cookies SYN TCP IPv4

Vérifiez que les machines hôtes du dispositif VMware utilisent des cookies SYN TCP IPv4.

Une attaque par saturation de type SYN TCP peut provoquer un déni de service en remplissant le tableau des connexions TCP d'un système avec des connexions dans l'état SYN_RCVD. Les cookies SYN empêchent le suivi d'une connexion jusqu'à réception de l'accusé de réception suivant en vérifiant que l'initiateur tente d'établir une connexion valide et qu'il n'est pas une source de saturation. Cette technique n'est pas totalement conforme aux normes. Elle est activée uniquement en cas de saturation et permet de protéger le système tout en continuant à traiter les demandes de service valides.

Procédure

- 1 Exécutez la commande `# cat /proc/sys/net/ipv4/tcp_syncookies` sur les machines hôtes du dispositif VMware pour vérifier qu'elles utilisent des cookies SYN TCP IPv4.

Si les machines hôtes sont configurées pour refuser le transfert IPv4, cette commande renvoie une valeur de 1 pour `/proc/sys/net/ipv4/tcp_syncookies`. Si les machines virtuelles sont correctement configurées, aucune autre action n'est nécessaire.

- 2 Si vous devez configurer un dispositif virtuel pour utiliser des cookies SYN TCP IPv4, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.

- 3 Localisez l'entrée contenant `net.ipv4.tcp_syncookies=1`.

Si la valeur de cette entrée n'est pas actuellement définie sur un ou si elle n'existe pas, ajoutez l'entrée ou mettez à jour l'entrée existante.

- 4 Enregistrez les modifications et fermez le fichier.

Refuser les annonces du routeur IPv6

Vérifiez que les machines hôtes VMware refusent l'acceptation des annonces du routeur et les redirections ICMP sauf exigence contraire du système.

IPv6 permet aux systèmes de configurer leurs périphériques réseau en utilisant automatiquement des informations provenant du réseau. Pour des raisons de sécurité, la configuration manuelle d'informations de configuration importantes est préférable à une acceptation sans authentification à partir du réseau.

Procédure

- 1 Exécutez la commande `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra | egrep "default|all"` sur les machines hôtes de dispositif VMware pour vérifier qu'elles refusent les annonces du routeur.

Si les machines hôtes sont configurées pour refuser les annonces du routeur IPv6, cette commande renvoie des valeurs 0 :

```
/proc/sys/net/ipv6/conf/all/accept_ra:0
/proc/sys/net/ipv6/conf/default/accept_ra:0
```

Si les machines hôtes sont correctement configurées, aucune autre action n'est nécessaire.

- 2 Si vous devez configurer une machine hôte pour refuser les annonces du routeur IPv6, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.

- 3 Recherchez les entrées suivantes.

```
net.ipv6.conf.all.accept_ra=0
net.ipv6.conf.default.accept_ra=0
```

Si ces entrées n'existent pas ou si leurs valeurs ne sont pas définies sur zéro, ajoutez-les ou mettez à jour les entrées existantes.

- 4 Enregistrez les modifications et fermez le fichier.

Refuser les sollicitations du routeur IPv6

Pour garantir la sécurité, il est recommandé de vérifier que les machines hôtes du dispositif VMware refusent les sollicitations du routeur IPv6, sauf si elles sont requises pour garantir le bon fonctionnement du système.

Le paramètre de sollicitations de routeur détermine le nombre de sollicitations de routeur envoyées lorsque vous mettez en place l'interface. Si les adresses sont attribuées de façon statique, il n'est pas nécessaire d'envoyer de sollicitations.

Procédure

- 1 Exécutez la commande `# grep [01] /proc/sys/net/ipv6/conf/*/router_sollicitations | egrep "default|all"` sur les machines hôtes du dispositif VMware pour vérifier qu'elles refusent les sollicitations du routeur IPv6.

Si les machines hôtes sont configurées pour refuser les annonces du routeur IPv6, cette commande renvoie ce qui suit :

```
/proc/sys/net/ipv6/conf/all/router_sollicitations:0
/proc/sys/net/ipv6/conf/default/router_sollicitations:0
```

Si les machines hôtes sont correctement configurées, aucune autre action n'est nécessaire.

- 2 Si vous devez configurer des machines hôtes pour refuser les sollicitations du routeur IPv6, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.
- 3 Recherchez les entrées suivantes.

```
net.ipv6.conf.all.router_sollicitations=0
net.ipv6.conf.default.router_sollicitations=0
```

Si les entrées n'existent pas ou si leurs valeurs ne sont pas définies sur zéro, ajoutez les entrées ou mettez à jour les entrées existantes.

- 4 Enregistrez les modifications et fermez le fichier.

Refuser la préférence du routeur IPv6 dans les sollicitations du routeur

Vérifiez que les machines hôtes du dispositif VMware refusent les sollicitations du routeur IPv6, sauf si elles sont requises pour garantir le bon fonctionnement du système.

La préférence du routeur dans le paramètre de sollicitations détermine les préférences de routeur. Si les adresses sont attribuées de façon statique, il n'est pas nécessaire de recevoir de préférence de routeur pour les sollicitations.

Procédure

- 1 Exécutez la commande `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_rtr_pref | egrep "default|all"` sur les machines hôtes du dispositif VMware pour vérifier qu'elles refusent les sollicitations du routeur IPv6.

Si les machines hôtes sont configurées pour refuser les annonces du routeur IPv6, cette commande renvoie ce qui suit :

```
/proc/sys/net/ipv6/conf/all/accept_ra_rtr_pref:0
/proc/sys/net/ipv6/conf/default/accept_ra_rtr_pref:0
```

Si les machines hôtes sont correctement configurées, aucune autre action n'est nécessaire.

- 2 Si vous devez configurer des machines hôtes pour refuser les sollicitations de route IPv6, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.
- 3 Recherchez les entrées suivantes.

```
net.ipv6.conf.all.accept_ra_rtr_pref=0
net.ipv6.conf.default.accept_ra_rtr_pref=0
```

Si les entrées n'existent pas ou si leurs valeurs ne sont pas définies sur zéro, ajoutez les entrées ou mettez à jour les entrées existantes en conséquence.

- 4 Enregistrez les modifications et fermez le fichier.

Refuser le préfixe du routeur IPv6

Vérifiez que les machines hôtes du dispositif VMware refusent les informations de préfixe du routeur IPv6, sauf si elles sont requises pour garantir le bon fonctionnement du système.

Le paramètre `accept_ra_pinfo` détermine si le système accepte les informations de préfixe en provenance du routeur. Si les adresses sont attribuées de façon statique, il n'est pas nécessaire de recevoir des informations de préfixe de routeur.

Procédure

- 1 Exécutez la commande `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_pinfo | egrep "default|all"` sur les machines hôtes du dispositif VMware pour vérifier qu'elles refusent les informations de préfixe du routeur IPv6.

Si les machines hôtes sont configurées pour refuser les annonces du routeur IPv6, cette commande renvoie ce qui suit.

```
/proc/sys/net/ipv6/conf/all/accept_ra_pinfo:0
/proc/sys/net/ipv6/conf/default/accept_ra_pinfo:0
```

Si les machines hôtes sont correctement configurées, aucune autre action n'est nécessaire.

- 2 Si vous devez configurer des machines hôtes pour refuser les informations de préfixe du routeur IPv6, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.

3 Recherchez les entrées suivantes.

```
net.ipv6.conf.all.accept_ra_pinfo=0
net.ipv6.conf.default.accept_ra_pinfo=0
```

Si les entrées n'existent pas ou si leurs valeurs ne sont pas définies sur zéro, ajoutez les entrées ou mettez à jour les entrées existantes.

4 Enregistrez les modifications et fermez le fichier.

Refuser les paramètres de limite de sauts d'annonce du routeur IPv6

Vérifiez que les machines hôtes du dispositif VMware refusent les paramètres de limite de sauts de routeur IPv6, sauf s'ils sont nécessaires.

Le paramètre `accept_ra_defrtr` détermine si le système accepte les paramètres de limite de sauts en provenance d'une annonce du routeur. Si vous définissez ce paramètre sur zéro, le routeur ne pourra pas modifier la limite de sauts IPv6 par défaut pour les paquets sortants.

Procédure

- 1 Exécutez la commande `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_defrtr | egrep "default|all"` sur les machines hôtes de dispositif VMware pour vérifier qu'elles refusent les paramètres de limite de sauts de routeur IPv6.

Si les machines hôtes sont configurées pour refuser les paramètres de limite de sauts de routeur IPv6, cette commande renvoie des valeurs 0.

```
/proc/sys/net/ipv6/conf/all/accept_ra_defrtr:0
/proc/sys/net/ipv6/conf/default/accept_ra_defrtr:0
```

Si les machines hôtes sont correctement configurées, aucune autre action n'est nécessaire.

- 2 Si vous devez configurer une machine hôte pour refuser les paramètres de limite de sauts de routeur IPv6, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.
- 3 Recherchez les entrées suivantes.

```
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.default.autoconf=0
```

Si les entrées n'existent pas ou si leurs valeurs ne sont pas définies sur zéro, ajoutez les entrées ou mettez à jour les entrées existantes.

4 Enregistrez les modifications et fermez le fichier.

Refuser les paramètres d'autoconfiguration d'annonce du routeur IPv6

Vérifiez que les machines hôtes du dispositif VMware refusent les paramètres d'autoconfiguration du routeur IPv6, sauf s'ils sont nécessaires.

Le paramètre `autoconf` détermine si les annonces du routeur peuvent entraîner l'attribution d'une adresse de monodiffusion globale à une interface par le système.

Procédure

- 1 Exécutez la commande `# grep [01] /proc/sys/net/ipv6/conf/*/autoconf | egrep "default|all"` sur les machines hôtes de dispositif VMware pour vérifier qu'elles refusent les paramètres d'autoconfiguration du routeur IPv6.

Si les machines hôtes sont configurées pour refuser les paramètres d'autoconfiguration du routeur IPv6, cette commande renvoie des valeurs 0.

```
/proc/sys/net/ipv6/conf/all/autoconf:0
/proc/sys/net/ipv6/conf/default/autoconf:0
```

Si les machines hôtes sont correctement configurées, aucune autre action n'est nécessaire.

- 2 Si vous devez configurer une machine hôte pour refuser les paramètres d'autoconfiguration du routeur IPv6, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.
- 3 Recherchez les entrées suivantes.

```
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.default.autoconf=0
```

Si les entrées n'existent pas ou si leurs valeurs ne sont pas définies sur zéro, ajoutez les entrées ou mettez à jour les entrées existantes.

- 4 Enregistrez les modifications et fermez le fichier.

Refuser les sollicitations de voisin IPv6

Vérifiez que vos machines hôtes de dispositif VMware refusent les sollicitations de voisin IPv6, sauf si elles sont nécessaires.

Le paramètre `dad_transmits` détermine le nombre de sollicitations de voisin devant être envoyées par adresse (globale et locale du lien) lorsque vous mettez en place une interface pour garantir que l'adresse souhaitée est unique sur le réseau.

Procédure

- 1 Exécutez la commande `# grep [01] /proc/sys/net/ipv6/conf/*/dad_transmits | egrep "default|all"` sur les machines hôtes de dispositif VMware afin de confirmer le refus des sollicitations de voisin IPv6.

Si les machines hôtes sont configurées pour refuser les sollicitations de voisin IPv6, cette commande renvoie des valeurs 0.

```
/proc/sys/net/ipv6/conf/all/dad_transmits:0
/proc/sys/net/ipv6/conf/default/dad_transmits:0
```

Si les machines hôtes sont correctement configurées, aucune autre action n'est nécessaire.

- 2 Si vous devez configurer une machine hôte pour refuser les sollicitations de voisin IPv6, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.

3 Recherchez les entrées suivantes.

```
net.ipv6.conf.all.dad_transmits=0
net.ipv6.conf.default.dad_transmits=0
```

Si les entrées n'existent pas ou si leurs valeurs ne sont pas définies sur zéro, ajoutez les entrées ou mettez à jour les entrées existantes.

4 Enregistrez les modifications et fermez le fichier.

Limitier le nombre maximal d'adresses IPv6

Assurez-vous que les machines hôtes du dispositif VMware limitent le nombre maximal d'adresses IPv6 au nombre minimal requis pour le fonctionnement du système.

Le paramètre relatif au nombre maximal d'adresses détermine le nombre d'adresses globales IPv6 de diffusion unicast disponibles sur chaque interface. La valeur par défaut est 16, mais vous devez définir le nombre exact d'adresses globales configurées de manière statique conformément à la configuration de votre système.

Procédure

- 1 Exécutez la commande `# grep [1] /proc/sys/net/ipv6/conf/*/max_addresses | egrep "default|all"` sur les machines hôtes du dispositif VMware pour vérifier que le nombre maximal d'adresses IPv6 est correctement limité.

Si les machines hôtes sont configurées de façon à limiter le nombre maximal d'adresses IPv6, cette commande renvoie 1.

```
/proc/sys/net/ipv6/conf/all/max_addresses:1
/proc/sys/net/ipv6/conf/default/max_addresses:1
```

Si les machines hôtes sont correctement configurées, aucune autre action n'est nécessaire.

- 2 Si vous devez configurer le nombre maximal d'adresses IPv6 sur les machines hôtes, ouvrez le fichier `/etc/sysctl.conf` dans un éditeur de texte.
- 3 Recherchez les entrées suivantes.

```
net.ipv6.conf.all.max_addresses=1
net.ipv6.conf.default.max_addresses=1
```

Si les entrées n'existent pas ou si leurs valeurs ne sont pas définies sur 1, ajoutez-les ou mettez à jour les entrées existantes.

- 4 Enregistrez les modifications et fermez le fichier.

Configuration des paramètres réseau pour l'hôte IaaS (Infrastructure en tant que service)

Pour garantir la sécurité, il est recommandé de configurer les paramètres de communication réseau sur votre machine hôte de composant IaaS (Infrastructure en tant que service) VMware, conformément aux exigences et aux directives VMware.

Définissez la configuration réseau de la machine hôte IaaS (Infrastructure en tant que service) pour prendre en charge des fonctions vRealize Automation complètes avec la sécurité appropriée.

Reportez-vous à [Sécurisation du composant IaaS \(Infrastructure en tant que service\)](#).

Configuration des ports et des protocoles

Pour garantir la sécurité, il est recommandé de configurer les ports et les protocoles de tous les dispositifs et composants vRealize Automation conformément aux directives de VMware.

Configurez les ports entrants et sortants des composants vRealize Automation, afin d'assurer le fonctionnement correct des composants système critiques. Désactivez tous les protocoles et ports inutiles. Reportez-vous à *Architecture de référence de vRealize Automation* dans la [documentation de VMware vRealize Automation](#).

Outil de ports et protocoles

L'outil de ports et protocoles vous permet d'afficher des informations sur le port pour une variété et une combinaison de produits VMware sur un seul tableau de bord. Vous pouvez également exporter les données sélectionnées à partir de l'outil pour une accessibilité hors ligne. L'outil de ports et protocoles prend actuellement en charge :

- vSphere
- vSAN
- NSX for vSphere
- vRealize Network Insight
- vRealize Operations Manager
- vRealize Automation

L'outil est disponible sur <https://ports.vmware.com/>.

Ports utilisateur requis

Pour garantir la sécurité, il est recommandé de configurer les ports utilisateur de vRealize Automation conformément aux directives de VMware.

Exposez les ports requis uniquement sur un réseau sécurisé.

SERVEUR	PORTS
Dispositif vRealize Automation	443, 8443

Ports requis par l'administrateur

Pour garantir la sécurité, il est recommandé de configurer les ports de l'administrateur de vRealize Automation conformément aux directives de VMware.

Exposez les ports requis uniquement sur un réseau sécurisé.

SERVEUR	PORTS
Serveur vRealize Application Services	5480

Ports du dispositif vRealize Automation

Pour garantir la sécurité, il est recommandé de configurer les ports entrants et sortants de dispositif vRealize Automation conformément aux recommandations de VMware.

Ports entrants

Configurez le nombre minimum de ports entrants requis pour dispositif vRealize Automation. Si nécessaire, configurez des ports facultatifs pour la configuration de votre système.

Tableau 1-1. Minimum de ports entrants requis

PORT	PROTOCOLE	COMMENTAIRES
443	TCP	Accès à la console vRealize Automation et aux appels d'API.
8443	TCP	Proxy de VMware Remote Console.
5480	TCP	Accès à l'interface de gestion du dispositif vRealize Automation.
5488, 5489	TCP	Interne. Utilisé par dispositif vRealize Automation pour les mises à jour.
5672	TCP	Messagerie RabbitMQ.
		Note Lors de la mise en cluster des instances de dispositif vRealize Automation, vous devrez configurer les ports ouverts 4369 et 25672.
40002	TCP	Requis pour le service vIDM. Protège par un pare-feu tout le trafic externe à l'exception du trafic provenant des autres nœuds de dispositif vRealize Automation en cas d'ajout à la configuration HA.

Si nécessaire, configurez les ports entrants facultatifs.

Tableau 1-2. Ports entrants facultatifs

PORT	PROTOCOLE	COMMENTAIRES
22	TCP	(Facultatif) SSH. Dans un environnement de production, désactivez le service SSH sur le port d'écoute 22 et fermez le port 22.
80	TCP	(Facultatif) Redirection vers le port 443.

Ports sortants

Configurez les ports sortants requis.

Tableau 1-3. Minimum de ports sortants requis

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.
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.
443	TCP	IaaS Manager Service sur HTTPS.

Si nécessaire, configurez les ports sortants facultatifs.

Tableau 1-4. Ports sortants facultatifs

PORT	PROTOCOLE	COMMENTAIRES
80	TCP	(Facultatif) Pour extraire des mises à jour logicielles. Vous pouvez télécharger et appliquer les mises à jour séparément.
123	TCP, UDP	(Facultatif) Pour la connexion directe au NTP au lieu d'utiliser l'heure de l'hôte.

Outil de ports et protocoles

L'outil de ports et protocoles vous permet d'afficher des informations sur le port pour une variété et une combinaison de produits VMware sur un seul tableau de bord. Vous pouvez également exporter les données sélectionnées à partir de l'outil pour une accessibilité hors ligne. L'outil de ports et protocoles prend actuellement en charge :

- vSphere
- vSAN
- NSX for vSphere
- vRealize Network Insight
- vRealize Operations Manager
- vRealize Automation

Les outils sont disponibles sur <https://ports.vmware.com/>.

Ports IaaS (Infrastructure en tant que service)

Pour garantir la sécurité, il est recommandé de configurer les ports entrants et sortants des composants IaaS (Infrastructure en tant que service) conformément aux directives de VMware.

Ports entrants

Configurez le nombre minimum requis de ports entrants pour les composants IaaS.

Tableau 1-5. Minimum de ports entrants requis

COMPOSANT	PORT	PROTOCOLE	COMMENTAIRES
Manager Service	443	TCP	Communication avec les composants IaaS et le dispositif vRealize Automation sur HTTPS. Tous les hôtes de virtualisation gérés par des agents proxy doivent également avoir le port TCP 443 ouvert pour le trafic entrant.

Ports sortants

Configurez le nombre minimum requis de ports sortants pour les composants IaaS.

Tableau 1-6. Minimum de ports sortants requis

COMPOSANT	PORT	PROTOCOLE	COMMENTAIRES
Tout	53	TCP, UDP	DNS.
Tout		TCP, UDP	DHCP.
Manager Service	443	TCP	Communication avec le dispositif vRealize Automation sur HTTPS.
Site Web	443	TCP	Communication avec Manager Service 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 de virtualisation sur HTTPS
Agent invité	443	TCP	Communication avec Manager Service sur HTTPS.
Manager Service, site Web	1433	TCP	MSSQL.

Si nécessaire, configurez les ports sortants facultatifs.

Tableau 1-7. Ports sortants facultatifs

COMPOSANT	PORT	PROTOCOLE	COMMENTAIRES
Tout	123	TCP, UDP	NTP est facultatif.

Audit et journalisation

Pour garantir la sécurité, il convient de configurer l'audit et la journalisation sur votre système vRealize Automation conformément aux recommandations de VMware.

La journalisation à distance vers un hôte de journalisation central fournit un stockage sécurisé pour les fichiers journaux. En collectant les fichiers journaux sur un hôte central, vous pouvez surveiller l'environnement avec un seul outil. En outre, vous pouvez effectuer une analyse cumulée et rechercher des signes de menaces telles que des attaques coordonnées sur plusieurs entités dans l'infrastructure. La connexion à un serveur de journalisation sécurisé et centralisé peut permettre d'éviter la falsification des journaux tout en fournissant un enregistrement d'audit à long terme.

Vérifier la sécurisation du serveur de journalisation à distance

Souvent, une fois que les pirates ont réussi à déjouer la sécurité de votre machine hôte, ils tentent de rechercher et de falsifier les fichiers journaux pour couvrir leurs traces et garder le contrôle sans être découverts. La sécurisation du serveur de journalisation à distance permet d'éviter la falsification des journaux.

Utiliser un serveur NTP autorisé

Assurez-vous que toutes les machines hôtes utilisent la même source d'heure relative (y compris le décalage de localisation applicable) et que vous pouvez mettre en corrélation la source d'heure relative avec une norme horaire acceptée telle que l'heure UTC (temps universel coordonné). Une approche stricte des sources d'heure vous permet de suivre et de corréler les actions des intrus lorsque vous passez en revue les fichiers journaux applicables. Des réglages d'heure incorrects compliquent l'analyse et la corrélation des fichiers journaux pour détecter d'éventuelles attaques et peuvent compromettre la précision des audits.

Utilisez au moins trois serveurs NTP de sources d'heure extérieures ou configurez sur un réseau approuvé quelques serveurs NTP locaux dont l'heure est obtenue à partir d'au moins trois sources d'heure extérieures.

Architecture de référence de vRealize Automation

L'architecture de référence décrit la structure et la configuration de déploiements types de vRealize Automation. En outre, elle fournit des informations sur des profils de haute disponibilité, d'évolutivité et de déploiement.

L'architecture de référence inclut des informations sur les composants suivants :

- VMware vRealize Automation
- VMware vRealize Business for Cloud

Pour la configuration logicielle requise, les installations et les plates-formes prises en charge, reportez-vous à la documentation de chaque produit.

Recommandations relatives au déploiement initial et à la configuration

Déployez et configurez tous les composants de VMware vRealize Automation conformément aux recommandations de VMware.

Gardez vos instances de vRealize Automation, de vRealize Business for Cloud et de vRealize Orchestrator dans le même fuseau horaire, leurs horloges étant synchronisées.

Installez vRealize Automation, vRealize Business for Cloud et vRealize Orchestrator sur le même cluster de gestion. Provisionnez les machines sur un cluster distinct du cluster de gestion afin que la charge de travail de l'utilisateur et la charge de travail du serveur puissent être isolées.

Déployez les agents proxy dans le même centre de données que celui du point de terminaison avec lequel ils communiquent. VMware déconseille de placer des DEM Workers dans des centres de données à distance à moins qu'un cas d'utilisation basé sur compétence de workflow express ne l'exige. Tous les composants, à l'exception des agents proxy et des DEM Workers, doivent être déployés dans le ou les mêmes centres de données dans un réseau métropolitain. La latence doit être inférieure à 5 millisecondes et la bande passante doit être d'au moins 1 Go/s entre les centres de données et le réseau métropolitain.

Pour obtenir plus d'informations, y compris une déclaration concernant le support, reportez-vous à l'[article 2134842 de la base de connaissances VMware](#) : *Installation de VMware vRealize Automation sur une instance distribuée avec plusieurs sites*.

Déploiement de vRealize Automation

Utilisez les recommandations relatives aux ressources de VMware comme point de départ pour la planification du déploiement de vRealize Automation.

Après les tests initiaux et le déploiement en production, continuez à surveiller les performances et allouez des ressources supplémentaires si nécessaire, de la manière décrite dans [Évolutivité de vRealize Automation](#).

Authentification

Lors de la configuration de vRealize Automation, vous pouvez utiliser le connecteur de gestion d'annuaires par défaut pour l'authentification des utilisateurs ou vous pouvez spécifier un fournisseur d'identité SAML préexistant pour prendre en charge une expérience d'authentification unique.

Si une authentification à deux facteurs est requise, vRealize Automation prend en charge l'intégration avec RSA SecurID. Lorsque ce point d'intégration est configuré, les utilisateurs sont invités à entrer leur ID et leur code secret.

Éléments à prendre en compte pour l'équilibrage de charge

Utiliser la méthode LRT (Least Response Time) ou Round-Robin pour équilibrer le trafic sur les dispositifs vRealize Automation et les serveurs Web de l'infrastructure. Activez l'affinité de session ou la fonctionnalité de session sticky pour diriger les demandes suivantes de chaque session unique vers le même serveur Web dans le pool d'équilibrage de charge.

Vous pouvez utiliser un équilibrage de charge pour gérer le basculement pour le service de gestionnaire, mais n'utilisez pas d'algorithme d'équilibrage de charge, car seulement un service de gestionnaire est actif à la fois. En outre, n'utilisez pas l'affinité de session lors de la gestion du basculement avec un équilibrage de charge.

Utiliser les ports 443 et 8444 lors de l'équilibrage de charge du dispositif vRealize Automation. Pour le site Web d'infrastructure et le service de gestionnaire d'infrastructure, seul le port 443 doit faire l'objet d'un équilibrage de charge.

Bien que vous puissiez utiliser d'autres équilibres de charge, NSX, le matériel F5 BIG-IP et F5 BIG-IP Virtual Edition sont testés et leur utilisation est recommandée.

Reportez-vous à la documentation de vRealize Automation pour plus d'informations sur la configuration des équilibres de charge.

Déploiement d'une base de données

Dans la version 7.0 et les versions ultérieures, vRealize Automation met automatiquement la base de données de dispositifs en clusters. Tous les nouveaux déploiements de la version 7.0 et des versions ultérieures doivent utiliser la base de données du dispositif interne. Les instances de vRealize Automation mises à niveau vers la version 7.1 ou version ultérieure doivent fusionner leurs bases de données externes dans la base de données du dispositif. Pour en savoir plus sur le processus de mise à niveau, consultez la documentation du produit vRealize Automation.

Pour des déploiements de production des composants d'infrastructure, utilisez un serveur de base de données dédié pour héberger les bases de données Microsoft SQL Server (MSSQL). vRealize Automation impose que les machines qui communiquent avec le serveur de base de données soient configurées pour utiliser Microsoft Distributed Transaction Coordinator (MSDTC). Par défaut, MSDTC a besoin du port 135 et des ports 1024 à 65535.

Pour plus d'informations concernant la modification des ports MSDTC par défaut, reportez-vous à l'[article 250367 de la base de connaissances Microsoft](#) : Configuration de Microsoft DTC (Distributed Transaction Coordinator) pour fonctionner avec un pare-feu.

L'hôte IaaS Manager Service doit être en mesure de résoudre le nom NETBIOS de l'hôte de la base de données IaaS SQL Server. S'il ne peut pas résoudre le nom NETBIOS, ajoutez le nom NETBIOS de SQL Server dans le fichier /etc/hosts de la machine Manager Service et redémarrez Manager Service.

vRealize Automation prend en charge les groupes SQL AlwaysON uniquement avec Microsoft SQL Server 2016. Lors de l'installation de SQL Server 2016, la base de données doit être créée en mode 100. Si vous utilisez une ancienne version de Microsoft SQL Server, utilisez une instance de cluster de basculement avec des disques partagés. Pour plus d'informations sur la configuration des groupes SQL AlwaysOn avec MSDTC, reportez-vous à <https://msdn.microsoft.com/fr-fr/library/ms366279.aspx>.

Configuration de la collecte de données

Les paramètres de collecte de données par défaut fournissent un bon point de départ pour la plupart des implémentations. Après le déploiement en production, continuez à surveiller les performances de la collecte des données pour déterminer si vous devez procéder à des ajustements.

agents proxy

Pour garantir des performances optimales, déployez les agents dans le même centre de données que le point de terminaison auquel ils sont associés. Vous pouvez installer des agents supplémentaires pour augmenter le débit et la simultanéité du système. Les déploiements distribués peuvent avoir plusieurs serveurs d'agents répartis à travers le monde.

Lorsque des agents sont installés dans le même centre de données que leur point de terminaison associé, vous pouvez constater une augmentation des performances de collecte des données de 200 pour cent en moyenne. La durée de collecte mesurée inclut uniquement le temps consacré au transfert des données entre l'agent proxy et le service de gestionnaire. Elle n'inclut pas le temps requis par le service de gestionnaire pour traiter les données.

Par exemple, vous déployez actuellement le produit sur un centre de données de Palo Alto et vous avez des points de terminaison vSphere à Palo Alto, Boston et Londres. Dans cette configuration, les agents proxy de vSphere sont déployés à Palo Alto, Boston et Londres pour leurs points de terminaison respectifs. Par contre, si les agents sont déployés uniquement à Palo Alto, il se peut que vous notiez une augmentation de 200 pour cent de la durée de collecte des données pour Boston et Londres.

Configuration de Distributed Execution Manager

En général, placez les DEM (Distributed Execution Manager) le plus près possible de l'hôte du gestionnaire de modèles. L'orchestrateur DEM doit disposer en tout temps d'une forte connectivité réseau au gestionnaire de modèles. Par défaut, le programme d'installation place les orchestrateurs DEM avec Manager Service. Créez deux instances de l'orchestrateur DEM, un pour le basculement, et deux instances de DEM Worker dans votre centre de données principal.

Si une instance de DEM Worker doit exécuter un workflow spécifique à un emplacement, installez l'instance à cet emplacement.

Attribuez des compétences aux workflows et aux DEM appropriés afin que ces workflows soient toujours exécutés par des DEM du même emplacement. Pour plus d'informations sur l'affectation de compétences aux workflows et aux DEM en utilisant la console du concepteur vRealize Automation, reportez-vous à la documentation sur l'extensibilité de vRealize Automation.

Pour obtenir des performances optimales, installez les DEM et les agents sur des machines distinctes. Pour obtenir des informations supplémentaires sur l'installation d'agents vRealize Automation, reportez-vous à [Installation d'agents](#).

vRealize Orchestrator

Utilisez l'instance intégrée de vRealize Orchestrator pour tous les nouveaux déploiements. Si nécessaire, les déploiements hérités peuvent continuer à utiliser une instance externe de vRealize Orchestrator. Consultez la page https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2147109 pour connaître la procédure à suivre pour augmenter la mémoire allouée à l'instance intégrée de vRealize Orchestrator.

Pour optimiser les performances du produit, consultez et appliquez les directives de configuration décrites dans le document *vRealize Orchestrator Coding Design Guide* avant d'importer du contenu vRealize Orchestrator dans des déploiements de production.

Éléments à prendre en compte pour le déploiement de vRealize Business for Cloud

Déployez vRealize Business for Cloud, anciennement nommé vRealize Business Standard Edition, conformément aux directives de VMware.

Éléments à prendre en compte pour l'équilibrage de charge

L'équilibrage de charge n'est pas pris en charge pour les connexions de collecte de données. Pour plus d'informations, reportez-vous à [Évolutivité de vRealize Automation](#). Dans le dispositif vRealize Business for Cloud pour les connexions clientes de l'interface utilisateur et de l'API, vous pouvez utiliser l'équilibrage de charge de vRealize Automation.

Évolutivité de vRealize Automation

Considérez tous les facteurs d'évolutivité applicables lors de la configuration de votre système vRealize Automation.

Utilisateurs

dispositif vRealize Automation est configuré pour synchroniser moins de 100 000 utilisateurs. Si votre système contient plus d'utilisateurs, vous devrez éventuellement ajouter de la mémoire à la gestion des annuaires de vRealize Automation. Pour plus d'informations sur l'ajout de mémoire à la gestion des annuaires, reportez-vous à [Ajouter de la mémoire à la gestion des annuaires](#).

Paramètres d'approvisionnement simultanées

VMware a évalué et réglé les paramètres par défaut dans vRealize Automation 7.5. Les valeurs par défaut suivantes s'appliquent aux nouvelles installations et aux mises à niveau vers vRealize Automation 7.5.

Paramètre par défaut	Détails
Réduction de la fréquence d'interrogation du service de gestionnaire de 10 secondes à 2 secondes dans <code>ManagerService.exe.config</code> .	<ul style="list-style-type: none"> ■ <code>RepositoryWorkflowTimerCallbackMilliseconds = 2000</code> ■ <code>MachineRequestTimerCallbackMilliseconds = 2000</code> ■ <code>MachineWorkflowCreationTimerCallbackMilliseconds = 2000</code>
Le nombre d'objets obtenus par intervalle d'interrogation a été exposé en tant que paramètre de configuration et augmenté de 10 à 100.	<ul style="list-style-type: none"> ■ <code>VirtualMachineObserverQueryCount = 100</code>
Augmentation de l'intervalle d'interrogation de l'agent proxy vSphere et du nombre maximal d'éléments de travail.	<ul style="list-style-type: none"> ■ <code>workitemTimeInterval = 00:00:05</code> ■ <code>workitemRetrievalCount = 100</code> ■ <code>activeQueueSize = 100</code>

Par défaut, vRealize Automation traite uniquement huit provisionnements concurrents par point de terminaison. Pour obtenir des informations sur l'augmentation de cette limite, reportez-vous à [Configuration de provisionnements de machines simultanés](#).

Distributed Execution Manager - Travailleurs

VMware recommande que tous les déploiements commencent avec au moins deux DEM-Workers. Dans la version 6.x, chaque DEM-Worker peut traiter 15 workflows simultanément. Ce nombre a été porté à 30 pour vRealize Automation 7.0 et versions ultérieures.

Si des machines sont personnalisées via des extrémités de workflow, vous devez prévoir 1 DEM-Worker par 20 machines qui seront provisionnés simultanément. Par exemple, un système prenant en charge 100 provisionnements simultanés doit disposer d'au moins 5 DEM-Workers.

Pour plus d'informations sur les Workers DEM et l'évolutivité, reportez-vous à [Analyse et réglage des performances de Distributed Execution Manager](#)

Évolutivité de la collecte des données

La durée d'exécution d'une collecte de données varie selon la capacité de la ressource de calcul, le nombre de machines sur la ressource de calcul ou le point de terminaison, le système actuel, la charge réseau et d'autres variables. Les performances évoluent à un rythme différent selon les types de collecte de données.

Chaque type de collecte de données a un intervalle par défaut que vous pouvez remplacer ou modifier. Les administrateurs d'infrastructure peuvent initier manuellement une collecte de données pour des points de terminaison source de l'infrastructure. Les administrateurs Fabric peuvent initier manuellement une collecte de données pour des ressources de calcul. Les valeurs suivantes constituent les intervalles par défaut de la collecte de données.

Tableau 1-8. Intervalles par défaut de la collecte de données

Type de collecte de données	intervalle par défaut
Inventaire	Toutes les 24 heures (quotidiennement)
État	Toutes les 15 minutes
Performances	Toutes les 24 heures (quotidiennement)

Analyse et réglage des performances

Lorsque le nombre de ressources collectant les données augmente, les temps de collecte peuvent devenir plus longs que les intervalles de collecte de données, notamment pour la collecte des données d'état. Pour déterminer si une collecte de données pour une ressource de calcul ou un point de terminaison s'exécute à temps ou est mis en file d'attente, reportez-vous à la page Collecte des données. La valeur du champ Dernière exécution peut afficher *En file d'attente* ou *En cours* à la place d'un horodatage de la fin de la dernière collecte de données. Si ce problème se produit, vous pouvez augmenter l'intervalle entre les collectes de données pour diminuer la fréquence de collecte des données.

Vous pouvez également augmenter la limite de collecte de données simultanée par agent. Par défaut, vRealize Automation limite les activités de collecte de données simultanées à deux par agent et met en file d'attente les demandes qui dépassent cette limite. Cette limite permet aux activités de collecte de données de se terminer rapidement sans incidence sur les performances globales. Vous pouvez augmenter la limite pour tirer parti de la collecte de données simultanée, mais vous devez trouver un compromis entre les avantages de cette option et la dégradation globale des performances.

Si vous augmentez la limite par agent configurée de vRealize Automation, vous pouvez augmenter un ou plusieurs de ces intervalles de délai d'exécution. Pour plus d'informations sur la configuration de la simultanéité de la collecte de données et des intervalles de délai d'exécution, reportez-vous à la documentation de l'administration du système vRealize Automation. La collecte des données du service de gestionnaire utilise le CPU de façon intensive. L'augmentation de la puissance de traitement de l'hôte du service de gestionnaire peut diminuer le temps requis pour une collecte de données globale.

La collecte de données pour Amazon Elastic Compute Cloud (Amazon AWS), en particulier, peut être très gourmande en ressources CPU, particulièrement si votre système collecte simultanément des données sur plusieurs régions et si les données n'ont pas été précédemment collectées sur ces régions. Ce type de collecte de données peut entraîner une dégradation globale des performances du site Web. Diminuez la fréquence de la collecte des données d'inventaire de Amazon AWS si celle-ci a un effet marqué sur les performances.

Évolutivité du traitement du workflow

Le temps de traitement moyen du workflow, à partir du moment où l'orchestrateur DEM commence à prétraiter le workflow jusqu'à la fin de l'exécution du workflow, augmente en fonction du nombre de workflows simultanés. Le volume du workflow est fonction du niveau d'activité de vRealize Automation, notamment les demandes de machines et certaines activités de collecte de données.

Configurer Manager Service pour un volume élevé de données

Si vous prévoyez d'utiliser un cluster VMware vSphere contenant un grand nombre d'objets (par exemple, 3 000 machines virtuelles ou plus), modifiez le fichier de configuration de Manager Service en sélectionnant des valeurs plus élevées. Si vous ne modifiez pas ce paramètre, les grandes collectes de données d'inventaire risquent d'échouer.

Modifiez la valeur par défaut des paramètres `ProxyAgentServiceBinding` et `maxStringContentLength` dans le fichier `ManagerService.exe.config`.

Procédure

- 1 Ouvrez le fichier `ManagerService.exe.config` dans un éditeur de texte.

En général, ce fichier se trouve à l'emplacement suivant : `C:\Program Files (x86)\VMware\VCAC\Server`.

- 2 Localisez le binding name et les lignes readerQuotas dans le fichier.

```
<binding name="ProxyAgentServiceBinding" maxReceivedMessageSize="13107200">
  <readerQuotas maxStringLength="13107200" />
```

Note Ne confondez pas ces deux lignes avec les lignes semblables contenant la chaîne suivante : `binding name = "ProvisionServiceBinding"`.

- 3 Remplacez les valeurs numériques attribuées aux attributs `maxReceivedMessageSize` et `maxStringLength` par des valeurs supérieures.

La taille optimale dépend du nombre d'objets supplémentaires que, selon vous, le cluster VMware vSphere contiendra dans le futur. Vous pouvez, par exemple, augmenter ces chiffres en appliquant un facteur de 10 pour les tests.

- 4 Enregistrez les modifications et fermez le fichier.
- 5 Redémarrez vRealize Automation Manager Service.

Analyse et réglage des performances de Distributed Execution Manager

Vous pouvez à tout moment afficher le nombre total de workflows en cours ou en attente sur une page État de Distributed Execution. Vous pouvez également utiliser la page Historique de workflow pour déterminer le temps nécessaire à l'exécution d'un workflow donné.

Si un grand nombre de workflows est en attente, ou si les workflows mettent plus de temps que prévu pour se terminer, ajoutez des instances supplémentaires de Distributed Execution Manager (DEM) Worker pour se charger des workflows. Chaque instance de DEM Worker peut traiter trente workflows simultanés. Les workflow excédentaires sont mis en file d'attente en vue de leur exécution.

Vous pouvez ajuster les planifications des workflows pour réduire le nombre de workflows démarrant simultanément. Ainsi, au lieu de planifier l'exécution de tous les workflows horaires pour que ceux-ci démarrent au début de l'heure, vous pouvez échelonner leurs heures d'exécution afin qu'ils ne se fassent pas concurrence pour les ressources DEM. Pour obtenir plus d'informations sur les workflows, consultez la documentation sur l'extensibilité de vRealize Automation.

Certains workflows, en particulier certains workflows personnalisés, peuvent faire une utilisation intensive du CPU. Si la charge du CPU sur les machines DEM Worker est élevée, envisagez d'augmenter la puissance de traitement de la machine DEM ou d'ajouter d'autres machines DEM à votre environnement.

Évolutivité de vRealize Business for Cloud

Configurez votre installation de vRealize Business for Cloud pour l'évolutivité conformément aux directives de VMware.

vRealize Business for Cloud peut faire évoluer jusqu'à 20 000 machines virtuelles dans dix instances de VMware vCenter Server. La première synchronisation de la collecte des données d'inventaire dure environ trois heures pour synchroniser 20 000 machines virtuelles dans trois instances de VMware vCenter Server. La synchronisation des statistiques de VMware vCenter Server prend environ une heure pour 20 000 machines virtuelles. Par défaut, le travail de calcul de coût s'exécute chaque jour et prend environ deux heures chaque fois pour 20 000 machines virtuelles.

Note Dans vRealize Business for Cloud 1.0, la configuration de dispositif virtuel par défaut peut prendre en charge jusqu'à 20 000 machines virtuelles. L'augmentation des limites du dispositif virtuel au-delà de sa configuration par défaut n'augmente pas le nombre de machines virtuelles qu'il peut prendre en charge.

Éléments à prendre en compte pour la configuration de la haute disponibilité vRealize Automation

Si vous avez besoin d'une robustesse système maximale, configurez votre système vRealize Automation pour une haute disponibilité conformément aux directives de VMware.

Dispositif vRealize Automation

Le dispositif vRealize Automation prend en charge la haute disponibilité active-active pour tous les composants à l'exception de la base de données du dispositif. À partir de la version 7.3, le basculement de base de données est automatique lorsque trois nœuds sont déployés et que la réplication synchrone est configurée entre deux nœuds. Lorsque le dispositif vRealize Automation détecte une panne de la base de données, il promeut un serveur de base de données adapté pour qu'il soit le contrôleur. Vous pouvez surveiller et gérer la base de données du dispositif sous l'onglet **Cluster** de l'interface de gestion du dispositif vRealize Automation.

Pour activer la haute disponibilité pour ces dispositifs, placez-les sous un équilibrage de charge. Pour plus d'informations, reportez-vous à [Configuration de votre équilibrage de charge](#). À partir de la version 7.0, la base de données des dispositifs et vRealize Orchestrator sont automatiquement mis en cluster et disponibles pour l'utilisation.

Gestion des annuaires vRealize Automation

Chaque instance du dispositif vRealize Automation inclut un connecteur qui prend en charge l'authentification de l'utilisateur, bien qu'un seul connecteur soit habituellement configuré pour exécuter la synchronisation d'annuaire. Le choix du connecteur devant faire office de connecteur de synchronisation est sans incidence. Afin de prendre en charge la haute disponibilité pour la fonctionnalité Gestion des annuaires, configurez un second connecteur qui correspond au second dispositif vRealize Automation. Ce connecteur doit se connecter au fournisseur d'identité et pointer vers la même instance d'Active Directory. Grâce à cette configuration, l'échec d'un dispositif est compensé par la reprise de la gestion de l'authentification de l'utilisateur par l'autre dispositif.

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

Pour plus d'informations sur la configuration de la gestion des annuaires pour la haute disponibilité, reportez-vous à [Configurer la gestion des annuaires pour la haute disponibilité](#).

Serveur Web d'infrastructure

Les composants du serveur Web de l'infrastructure prennent tous en charge la haute disponibilité active-active. Pour activer la haute disponibilité pour ces composants, placez-les sous un équilibrage de charge.

Service de gestionnaire d'infrastructure

Le composant du service de gestionnaire prend en charge la haute disponibilité active-passive. Pour activer la haute disponibilité pour ce composant, placez deux services de gestionnaire sous un équilibrage de charge. Dans vRealize Automation 7.3 et versions ultérieures, le basculement est automatique.

Si le service de gestionnaire échoue, arrêtez le service Windows, s'il n'est pas déjà arrêté sous l'équilibrage de charge. Activez le service de gestionnaire passif et redémarrez le service Windows sous l'équilibrage de charge. Reportez-vous à [Installer le service Active Manager Service](#).

Agents

Les agents prennent en charge la haute disponibilité active-active. Pour plus d'informations sur la configuration d'agents pour la haute disponibilité, reportez-vous à la documentation sur la configuration de vRealize Automation. Vérifiez le service cible pour la haute disponibilité.

Distributed Execution Manager Worker

Un Distributed Execution Manager (DEM) s'exécutant sous le rôle Worker prend en charge la haute disponibilité active-active. Si une instance de DEM Worker échoue, l'orchestrateur DEM détecte la panne et annule les workflows que l'instance de DEM Worker exécute. Lorsque l'instance de DEM Worker revient en ligne, elle détecte que l'orchestrateur DEM a annulé les workflows de l'instance et cesse de les exécuter. Pour éviter que les workflows soient annulés prématurément, laissez une instance de DEM Worker hors ligne pendant plusieurs minutes avant d'annuler ses workflows.

Orchestrateur Distributed Execution Manager

Les DEM s'exécutant sous le rôle Orchestrateur prennent en charge la haute disponibilité active-active. Lorsqu'un orchestrateur DEM démarre, il recherche un autre orchestrateur DEM en cours d'exécution.

- S'il ne trouve aucune instance d'orchestrateur DEM en cours d'exécution, il commence à s'exécuter comme l'orchestrateur DEM principal.
- S'il trouve un autre orchestrateur DEM en cours d'exécution, il surveille l'autre orchestrateur DEM principal pour détecter une panne.
- S'il détecte une panne, il prend la main comme instance principale.

Lorsque l'instance principale précédente revient en ligne, elle détecte qu'un autre orchestrateur DEM a pris son rôle comme instance principale et surveille l'instance de l'orchestrateur principale pour détecter une éventuelle panne.

Serveur de base de données MSSQL pour les composants d'infrastructure

vRealize Automation prend en charge les groupes SQL AlwaysON uniquement avec Microsoft SQL Server 2016. Lors de l'installation de SQL Server 2016, la base de données doit être créée en mode 100. Si vous utilisez une ancienne version de Microsoft SQL Server, utilisez une instance de cluster de basculement avec des disques partagés. Pour plus d'informations sur la configuration des groupes SQL AlwaysOn avec MSDTC, reportez-vous à l'article de Microsoft à l'adresse <https://msdn.microsoft.com/en-us/library/ms366279.aspx>.

vRealize Orchestrator

Une instance hautement disponible intégrée de vRealize Orchestrator est fournie comme partie intégrante du dispositif vRealize Automation.

Éléments à prendre en compte pour la haute disponibilité de vRealize Business for Cloud

Utilisez la fonctionnalité VMware vSphere HA pour le dispositif vRealize Business for Cloud.

Pour configurer la fonctionnalité VMware vSphere HA sur l'hôte ESXi VMware, reportez-vous à la documentation de vCenter Server et Gestion des hôtes.

Spécifications matérielles et capacité maximale de vRealize Automation

Installez les composants adaptés à votre configuration et à vos besoins en capacité sur chaque profil de serveur vRealize Automation de votre environnement.

Rôle de serveur	Composants	Spécifications du matériel requis	Spécifications du matériel recommandé
Dispositif vRealize Automation	Services vRealize Automation, vRealize Orchestrator, base de données des dispositifs vRealize Automation	CPU : 4 vCPU RAM : 18 Go (pour plus d'informations, voir Évolutivité de vRealize Automation.) Disque : 140 Go Réseau : 1 Go/s	Identiques aux spécifications matérielles requises.
Serveur Infrastructure Core	Site Web, service de gestionnaire, DEM Orchestrator, DEM Worker, agent Proxy	CPU : 4 vCPU RAM : 8 Go Disque : 40 Go Réseau : 1 Go/s	Identiques aux spécifications matérielles requises.
Serveur Web d'infrastructure	Site Web	CPU : 2 vCPU RAM : 8 Go Disque : 40 Go Réseau : 1 Go/s	CPU : 2 vCPU RAM : 8 Go Disque : 40 Go Réseau : 1 Go/s
Serveur de gestionnaire d'infrastructure	Service de gestionnaire, DEM Orchestrator	CPU : 2 vCPU RAM : 8 Go Disque : 40 Go Réseau : 1 Go/s	CPU : 2 vCPU* RAM : 8 Go Disque : 40 Go Réseau : 1 Go/s * 4 vCPU lors de l'exécution de plus de 100 provisionnements simultanés.
Infrastructure Web/serveur de gestionnaire	Infrastructure Web/serveur de gestionnaire	CPU : 2 vCPU RAM : 8 Go Disque : 40 Go Réseau : 1 Go/s	CPU : 2 vCPU RAM : 8 Go Disque : 40 Go Réseau : 1 Go/s
Serveur DEM d'infrastructure	(un ou plusieurs) DEM Workers	CPU : 2 vCPU RAM : 8 Go Disque : 40 Go Réseau: 1 Go/s par DEM Worker	CPU : 2 vCPU* RAM : 8 Go Disque : 40 Go Réseau: 1 Go/s par DEM Worker * 4 vCPU en cas d'exécution de plus de 100 provisionnements simultanés.
Serveur d'agent d'infrastructure	(un ou plusieurs) agents Proxy	CPU : 2 vCPU RAM : 8 Go Disque : 40 Go Réseau : 1 Go/s	CPU : 2 vCPU RAM : 8 Go Disque : 40 Go Réseau : 1 Go/s

Rôle de serveur	Composants	Spécifications du matériel requis	Spécifications du matériel recommandé
Serveur de base de données MSSQL	Base de données de l'infrastructure	CPU : 2 vCPU RAM : 8 Go Disque : 40 Go Réseau : 1 Go/s	CPU : 8 vCPU RAM : 16 Go Disque : 80 Go Réseau : 1 Go/s
Dispositif vRealize Business for Cloud	Services du dispositif vRealize Business for Cloud Serveur de base de données vRealize Business for Cloud	CPU : 2 vCPU RAM : 4 Go Disque : 50 Go Réseau : 1 Go/s	Identiques aux spécifications matérielles requises.

Capacités maximales recommandées pour vRealize Automation

Les valeurs maximales de capacité des ressources présentées ci-après s'appliquent au profil de déploiement à grande échelle de vRealize Automation.

Tableau 1-9. Capacités maximales de ressources dans vRealize Automation

Paramètre		Valeur maximale
Locataire		100
Points de terminaison vSphere		45* * Maximum de 25 agents vCenter par serveur.
Ressources de calcul		200
Machines gérées		75 000
Pic de demandes simultanées		
	Constante	100
	Salves	250
Groupes d'activité		5 000 Avec 10 utilisateurs uniques par groupe d'activité et aucun utilisateur membre de plus de 50 groupes d'activité.
Réservations		14 000 Avec 3 réservations par groupe d'activité.
Blueprints		
	CBP uniquement	6 000
	CBP + XaaS	8 000
Éléments du catalogue		
	Entre les locataires	4 000
	Dans un locataire unique	6 000

Tableau 1-9. Capacités maximales de ressources dans vRealize Automation (suite)

Paramètre	Valeur maximale	
Synchronisation d'utilisateur/de groupe avec 18 Go de mémoire par défaut	Nombre d'utilisateurs	95 000
	Nombre de groupes	20 000 Chaque groupe contient 4 utilisateurs, y compris un niveau d'imbrication.
Utilisateur/groupe avec mémoire portée à 30 Go	Nombre d'utilisateurs	100 000
	Nombre de groupes	750 Chaque groupe contient 4 000 utilisateurs et chaque utilisateur est dans 30 groupes.

Configuration requise pour un petit déploiement de vRealize Automation

Un petit déploiement de vRealize Automation comprend des systèmes de 10 000 machines gérées ou moins, et inclut les machines virtuelles, les équilibres de charges et les configurations de port appropriés. Le petit déploiement sert de point de départ pour un déploiement de vRealize Automation qui vous permet d'évoluer facilement vers un déploiement moyen ou grand.

Lors du déploiement de vRealize Automation, utilisez le processus de déploiement d'entreprise pour fournir un site Web d'infrastructure et une adresse de service de gestionnaire distincts.

Support

Un petit déploiement peut prendre en charge les éléments suivants.

- 10 000 machines gérées
- 500 éléments du catalogue
- 10 provisionnements de machines simultanés

Configuration requise

Un petit déploiement doit être configuré avec les composants appropriés.

- Dispositif vRealize Automation : vrava-1.ra.local
- Serveur Infrastructure Core : inf-1.ra.local.
- Serveur de base de données MSSQL : mssql.ra.local
- Dispositif vRealize Business for Cloud : vrb.ra.local

Entrées DNS

Entrée DNS	Pointe vers
vrava.ra.local	vrava-1.ra.local
web.ra.local	inf.ra.local
manager.ra.local	inf.ra.local

Certificats

Les noms d'hôtes utilisés dans ce tableau sont uniquement des exemples.

Rôle de serveur	CN ou SAN
Dispositif vRealize Automation	SAN contient vra.va.sqa.local et vra.va-1.sqa.local
Serveur Infrastructure Core	SAN contient web.ra.local, managers.ra.local et inf-1.ra.local
Serveur vRealize Business for Cloud	CN = vrb.ra.local

Ports

Les utilisateurs nécessitent l'accès à certains ports. Tous les ports répertoriés sont des ports par défaut.

Rôle de serveur	Port
Dispositif vRealize Automation	443, 8444. Le port 8444 est requis pour la console distante de machines virtuelles. Le port 8283 est requis pour accéder au centre de contrôle de vRealize Orchestrator.

Les administrateurs nécessitent l'accès à certains ports, en complément des ports requis par les utilisateurs.

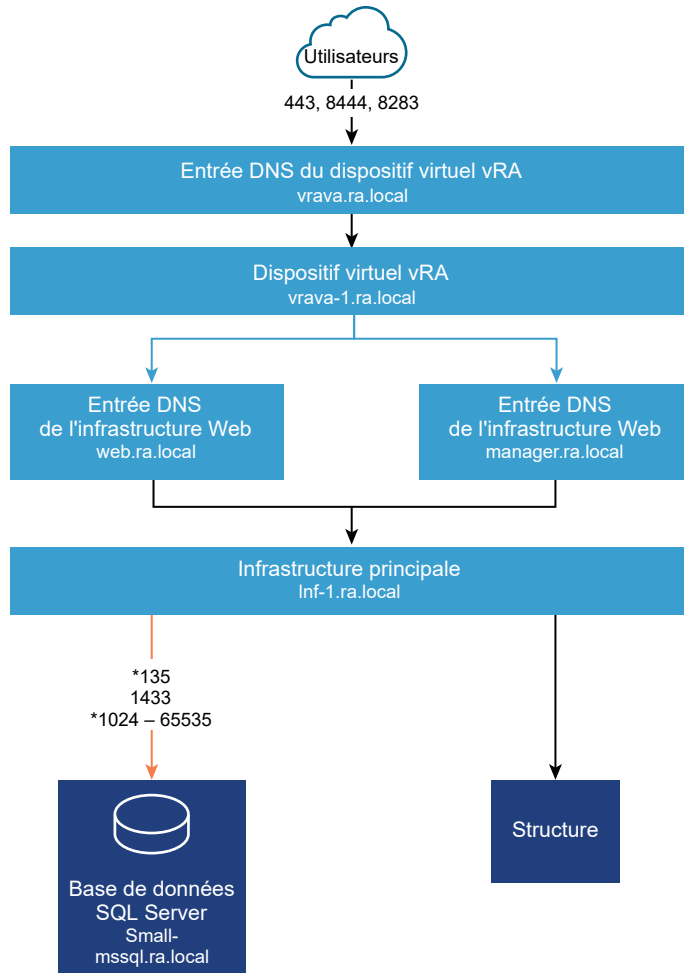
Rôle de serveur	Port
Dispositif vRealize Automation	5480, 8443. Le port 8443 est utilisé pour la configuration avancée de gestion des identités. VMware Identity Manager vers Active Directory : 389, 636, 3268, 3269 VMware Identity Manager vers Domain Controller : 88, 464, 135
vRealize Business for Cloud	5480

Rôle de serveur	Ports entrants	Ports sortants des services/système
Dispositif vRealize Automation	HTTPS : 443 Configuration d'adaptateur : 8443 Proxy de console distante : 8444 SSH : 22 Interface de gestion du dispositif vRealize Automation : 5480	LDAP : 389 LDAPS : 636 VMware ESXi : 902 Infrastructure Core nécessite un accès au port 443 du point de terminaison vSphere pour obtenir un ticket pour VMware Remote Console. Le dispositif vRealize Automation nécessite un accès au port 902 de l'hôte ESXi pour transmettre par proxy le trafic au consommateur. Serveur Infrastructure Core : 443 Authentification Kerberos : 88 Renouvellement du mot de passe de l'objet ordinateur : 464
Serveur Infrastructure Core	HTTPS : 443 MSDTC : 135, 1024 - 65535. Pour savoir comment mieux cibler cette plage, reportez-vous à la section de déploiement de la base de données de Déploiement de vRealize Automation .	Dispositif virtuel vRealize Automation : 443, 5480 Point de terminaison vSphere : 443 Infrastructure Core nécessite un accès au port 443 du point de terminaison vSphere pour obtenir un ticket pour VMware Remote Console. Le dispositif vRealize Automation nécessite un accès au port 902 de l'hôte ESXi pour transmettre par proxy le trafic au consommateur. MSSQL : 135, 1433, 1024 à 65535. MSDTC : 135, 1024 - 65535. Pour savoir comment mieux cibler cette plage, reportez-vous à la section de

Rôle de serveur	Ports entrants	Ports sortants des services/système
		déploiement de la base de données de Déploiement de vRealize Automation .
Serveur de base de données MSSQL	MSSQL : 1433 MSDTC : 135, 1024 - 65535. Pour savoir comment mieux cibler cette plage, reportez-vous à la section de déploiement de la base de données de Déploiement de vRealize Automation .	Serveur Infrastructure Core : 135, 1024 à 65535. Pour savoir comment mieux cibler cette plage, reportez-vous à la section de déploiement de la base de données de Déploiement de vRealize Automation . MSDTC : 135, 1024 - 65535. Pour savoir comment mieux cibler cette plage, reportez-vous à la section de déploiement de la base de données de Déploiement de vRealize Automation .
Dispositif vRealize Business for Cloud	HTTPS : 443 SSH : 22 Interface de gestion du dispositif vRealize Automation : 5480	Dispositif virtuel vRealize Automation : 443 Infrastructure Core : 443
Catalogue global		Catalogue global : 3268, 3269

Encombres minimaux

Figure 1-3. Encombres minimaux pour une petite configuration de vRealize Automation



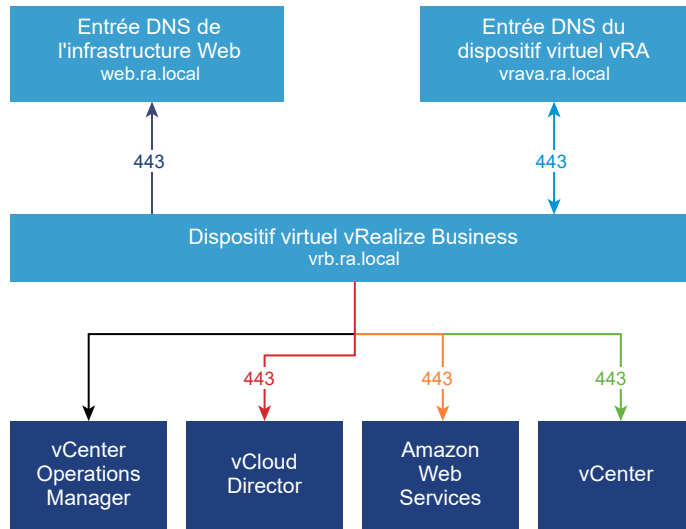
Non affiché :
tous les systèmes d'infrastructure
nécessitent un accès au port 5480 de
tous les dispositifs vRealize Appliance
pour la collecte de journaux (vRA >
Cluster > Collecter les journaux sur le
dispositif virtuel : 5480) pour fonctionner.

Pour la console distante de machines
virtuelles, vRealize Appliance nécessite
un accès au port 902 de VMware ESXi
et le serveur Infrastructure Core
nécessite un accès au port 443 du
point de terminaison de vSphere.

*Reportez-vous à la section Déploiement de base de données pour découvrir comment mieux cibler cette plage

En outre, une communication bidirectionnelle est requise.

Figure 1-4. Encombres minimaux pour une petite configuration de vRealize Business for Cloud



Configuration requise d'un déploiement moyen de vRealize Automation

Un déploiement moyen de vRealize Automation comprend des systèmes de 30 000 machines gérées ou moins, et inclut les machines virtuelles, les équilibres de charges et les configurations de ports appropriés.

Support

Un déploiement moyen peut prendre en charge les éléments suivants.

- 30 000 machines gérées
- 1 000 éléments de catalogue
- 50 provisionnements de machines simultanés

Configuration requise

Un déploiement moyen doit répondre à la configuration système requise appropriée.

Dispositifs virtuels

- Dispositif vRealize Automation 1 : vrava-1.ra.local
- Dispositif vRealize Automation 2 : vrava-2.ra.local
- Dispositif vRealize Automation 3 : vrava-3.ra.local
- Dispositif vRealize Business for Cloud : vrb.ra.local

Machines virtuelles Windows Server

- Serveur de gestionnaire/Web d'infrastructure 1 (Web active ou DEM-O, gestionnaire actif) : inf-1.ra.local

- Serveur de gestionnaire/Web d'infrastructure 2 (Web active ou DEM-O, gestionnaire passif) : inf-2.ra.local
- Serveur DEM d'infrastructure 1 : dem-1.ra.local
- Serveur DEM d'infrastructure 2 : dem-2.ra.local
- Serveur d'agent d'infrastructure 1 : agent-1.ra.local
- Serveur d'agent d'infrastructure 2 : agent-2.ra.local

Serveurs de base de données

- Instance de cluster de basculement MSSQL : mssql.ra.local

Équilibrages de charge

- Équilibrage de charge de dispositif vRealize Automation : med-vrava.ra.local
- Équilibrage de charge du Web d'Infrastructure : med-web.ra.local
- Équilibrage de charge de service de gestionnaire d'infrastructure : med-manager.ra.local

Certificats

Les noms d'hôtes qui sont utilisés dans ce tableau sont fournis à titre d'exemple uniquement.

Rôle de serveur	CN ou SAN
Dispositif vRealize Automation	SAN contient les noms d'hôtes suivants : <ul style="list-style-type: none"> ■ vrava.ra.local ■ vrava-1.ra.local ■ vrava-2.ra.local
Serveur Web d'infrastructure ou de gestionnaire	SAN contient les noms d'hôtes suivants : <ul style="list-style-type: none"> ■ web.ra.local ■ manager.ra.local ■ inf-1.ra.local ■ inf-2.ra.local
Dispositif vRealize Business for Cloud	CN = vrb.ra.local

Ports

Les utilisateurs nécessitent l'accès à certains ports. Tous les ports répertoriés sont des ports par défaut.

Rôle de serveur	Port
Équilibrage de charge du dispositif vRealize Automation	443, 8444. Le port 8444 est requis pour la console distante de machines virtuelles.

Les administrateurs nécessitent l'accès à certains ports, en complément des ports requis par les utilisateurs.

Rôle de serveur	Port
Interface de gestion du dispositif vRealize Automation	5480, 8443. Le port 8443 est destiné à la configuration avancée de gestion des identités. VMware Identity Manager vers Active Directory : 389, 636, 3268, 3269 VMware Identity Manager vers Domain Controller : 88, 464, 135
Centre de contrôle de vRealize Appliance Orchestrator	8283
Serveur vRealize Business for Cloud	5480

Le tableau suivant répertorie les communications entre les applications.

Rôle de serveur	Ports entrants	Ports sortants pour service ou système
Dispositif vRealize Automation	HTTPS : Configuration d'adaptateur : 8443 Proxy de console distante : 8444 Postgres : 5432 RabbitMQ : 4369, 25672, 5671, 5672 Elasticsearch : 9300, 40002, 40003 Stomp : 61613 SSH : 22	LDAP : 389 LDAPS : 636 Dispositif vRealize Automation (tous les autres) : 5432, 4369, 25672, 5671, 5672, 9300, 40002, 40003 Équilibrage de charge de Web d'infrastructure vRealize Automation : 443 VMware ESXi : 902. Le gestionnaire ou Web d'infrastructure nécessite un accès au port 443 du point de terminaison vSphere pour obtenir un ticket pour la console distante de machines virtuelles. Le dispositif vRealize Automation nécessite un accès au port 902 de l'hôte ESXi pour transmettre via proxy les données de console à l'utilisateur. Authentification Kerberos : 88 Renouvellement du mot de passe de l'objet ordinateur : 464
Serveur de gestionnaire/Web d'infrastructure	HTTPS : 443 MSDTC : 135, 1024-65535. Pour savoir comment mieux cibler cette plage, reportez-vous à la section de déploiement de la base de données de Déploiement de vRealize Automation .	Équilibrage de charge du dispositif vRealize Automation : 443 Équilibrage de charge de Web d'infrastructure vRealize Automation : 443 Dispositif vRealize Automation : 5480. Point de terminaison vSphere : 443. Le gestionnaire ou Web d'infrastructure nécessite un accès au port 443 du point de terminaison vSphere pour obtenir un ticket pour la console distante de machines virtuelles. Le dispositif vRealize Automation nécessite un accès au port 902 de l'hôte ESXi pour transmettre via proxy les données de console à l'utilisateur. MSSQL : 135, 1433, 1024 à 65535. Pour savoir comment mieux cibler cette plage, reportez-vous à la section de déploiement de la base de données de Déploiement de vRealize Automation .

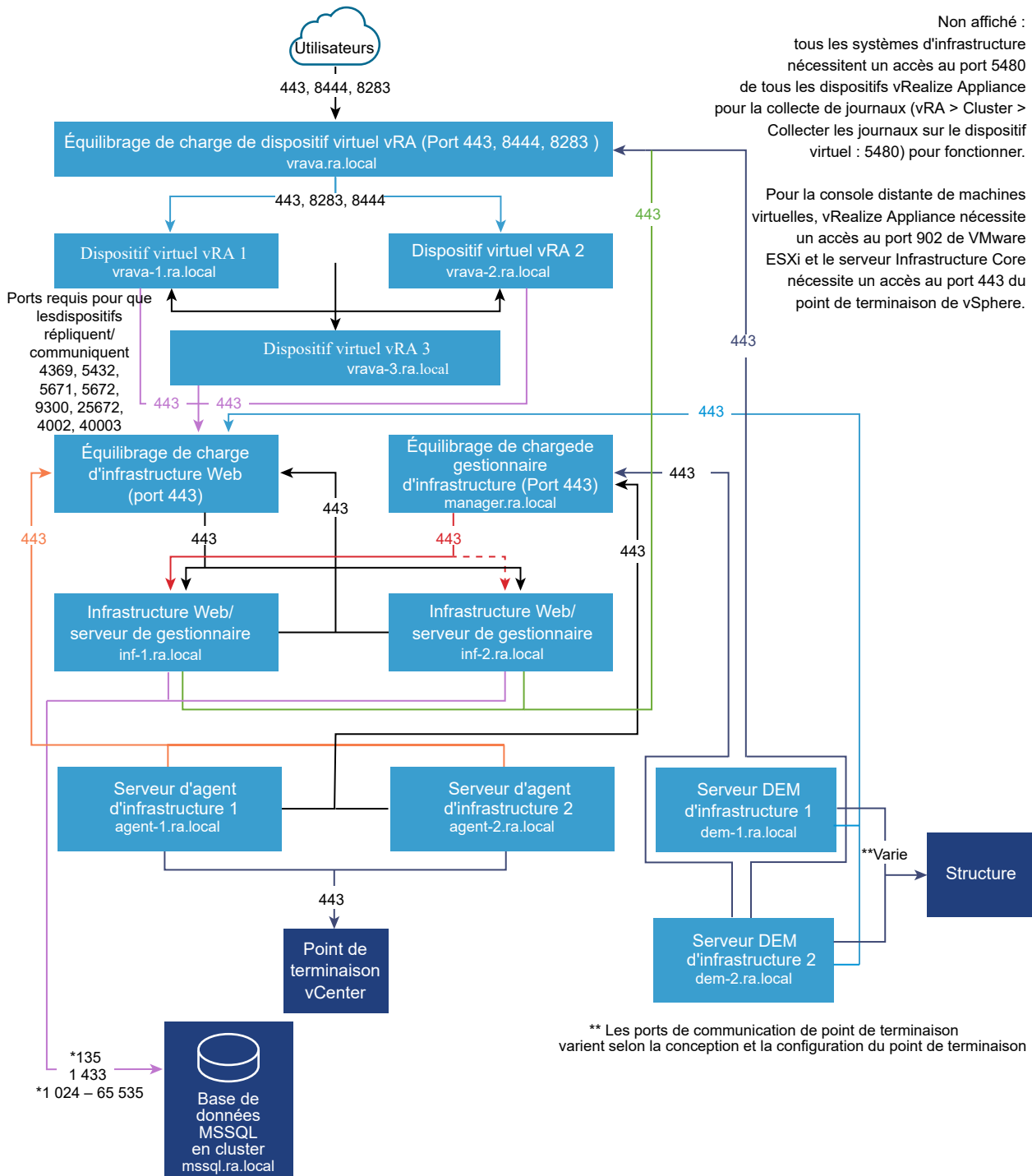
Rôle de serveur	Ports entrants	Ports sortants pour service ou système
Serveur DEM d'infrastructure	SO	Équilibrage de charge du dispositif vRealize Automation : 443 Équilibrage de charge de Web d'infrastructure vRealize Automation : 443 Équilibrage de charge de gestionnaire d'infrastructure vRealize Automation : 443 Dispositif vRealize Automation : 5480.
Serveur d'agent d'infrastructure	SO	Équilibrage de charge de Web d'infrastructure vRealize Automation : 443 Équilibrage de charge de gestionnaire d'infrastructure vRealize Automation : 443 Dispositif vRealize Automation : 5480.
Serveur de base de données MSSQL	MSSQL : 1433 MSDTC : 135, 1024 - 65535. Pour savoir comment mieux cibler cette plage, reportez-vous à la section de déploiement de la base de données de Déploiement de vRealize Automation .	Serveur de gestionnaire/Web d'infrastructure : 135, 1024 - 65535. Pour savoir comment mieux cibler cette plage, reportez-vous à la section de déploiement de la base de données de Déploiement de vRealize Automation .
Serveur vRealize Business for Cloud	HTTPS : 443 SSH : 22 Interface de gestion du dispositif vRealize Automation : 5480	Équilibrage de charge du dispositif vRealize Automation : 443 Équilibrage de charge de Web d'infrastructure vRealize Automation : 443
Catalogue global		Catalogue global : 3268, 3269

Les équilibrages de charge nécessitent un accès par les ports suivants.

Équilibrage de charge	Ports équilibrés
Équilibrage de charge du dispositif vRealize Automation	443, 8444
Équilibrage de charge de Web d'infrastructure vRealize Automation	443
Équilibrage de charge du service de gestionnaire d'infrastructure vRealize Automation	443

Graphiques

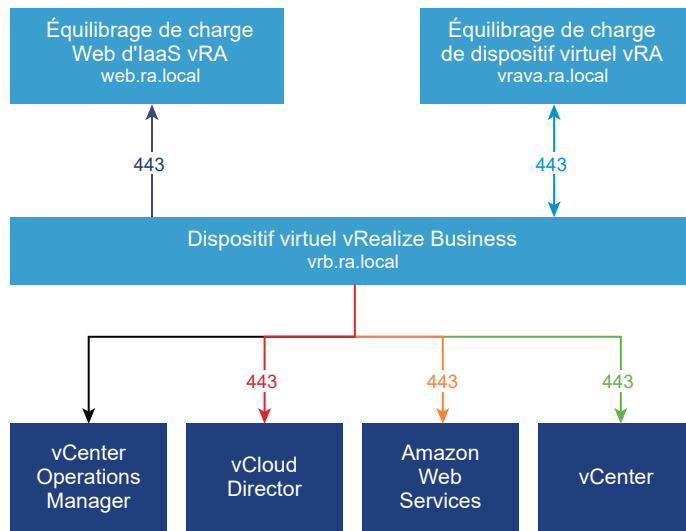
Figure 1-5. Encombrement minimal d'une configuration moyenne de vRealize Automation



*Reportez-vous à la section Déploiement de base de données pour découvrir comment mieux cibler cette page

En outre, une communication bidirectionnelle est requise.

Figure 1-6. Encombrement minimal d'un déploiement moyen de vRealize Business for Cloud



Configuration requise pour un grand déploiement de vRealize Automation

Un grand déploiement de vRealize Automation comprend des systèmes de 75 000 machines gérées ou moins, et inclut les machines virtuelles, les équilibres de charges et les configurations de ports appropriés.

Support

Un grand déploiement peut prendre en charge les éléments suivants.

- 75 000 machines gérées
- 2 500 éléments de catalogue
- 100 provisionnements de machines simultanés

Configuration requise

Un grand déploiement doit répondre à la configuration système requise appropriée.

Dispositifs virtuels

- Dispositif vRealize Automation 1 : vrava-1.ra.local
- Dispositif vRealize Automation 2 : vrava-2.ra.local
- Dispositif vRealize Automation 2 : vrava-3.ra.local
- Dispositif vRealize Business for Cloud : vrb.ra.local

Machines virtuelles Windows Server

- Serveur Web d'infrastructure 1 : web-1.ra.local
- Serveur Web d'infrastructure 2 : web-2.ra.local

- Serveur de gestionnaire d'infrastructure 1 : manager-1.ra.local
- Serveur de gestionnaire d'infrastructure 2 : manager-2.ra.local
- Serveur DEM d'infrastructure 1 : dem-1.ra.local
- Serveur DEM d'infrastructure 2 : dem-2.ra.local
- Serveur d'agent d'infrastructure 1 : agent-1.ra.local
- Serveur d'agent d'infrastructure 2 : agent-2.ra.local
- Base de données MSSQL en cluster : mssql.ra.local

Équilibrages de charge

- Équilibrage de charge du dispositif vRealize Automation : vrava.ra.local
- Équilibrage de charge de Web d'infrastructure : web.ra.local
- Équilibrage de charge du service du gestionnaire d'infrastructure : manager.ra.local

Certificats

Les noms d'hôtes utilisés dans ce tableau sont uniquement des exemples.

Rôle de serveur	CN ou SAN
Dispositif vRealize Automation	SAN contient les noms d'hôtes suivants : <ul style="list-style-type: none"> ■ vrava.ra.local ■ vrava-1.ra.local ■ vrava-2.ra.local
Serveur Web d'infrastructure	SAN contient les noms d'hôtes suivants : <ul style="list-style-type: none"> ■ web.ra.local ■ web-1.ra.local ■ web-2.ra.local
Serveur de gestionnaire d'infrastructure	SAN contient les noms d'hôtes suivants : <ul style="list-style-type: none"> ■ manager.ra.local ■ manager-1.ra.local ■ manager-2.ra.local
Dispositif vRealize Business for Cloud	CN = vrb.ra.local

Ports

Les utilisateurs nécessitent l'accès à certains ports. Tous les ports répertoriés sont des ports par défaut.

Rôle de serveur	Port
Équilibrage de charge du dispositif vRealize Automation	443, 8444, 8283 Port 8444 est requis pour le VMware Remote Console Port 8382 est requis pour le centre de contrôle vRealize Orchestrator.

Les administrateurs nécessitent l'accès à certains ports, en complément des ports requis par les utilisateurs.

Rôle de serveur	Port
Dispositif vRealize Automation	5480, 8283, 8443. Le port 8443 est utilisé pour la configuration avancée de gestion des identités. VMware Identity Manager vers Active Directory : 389, 636, 3268, 3269 VMware Identity Manager vers Domain Controller : 88, 464, 135
Serveur vRealize Business for Cloud	5480

Le système doit prendre en charge les communications appropriées entre les applications.

Rôle de serveur	Ports entrants	Ports sortants pour service ou système
vRealize Automation		
Dispositif vRealize Automation	HTTPS : 443 Configuration d'adaptateur : 8443 Proxy de console distante : 8444 Postgres : 5432 Rabbit MQ : 4369, 25672, 5671, 5672 ElasticSearch : 9300, 40002, 40003 Stomp : 61613 SSH : 22 Control-Center : 8283	LDAP : 389 LDAPS : 636 Dispositif vRealize Automation : 5432, 4369, 25672, 5671, 5672, 9300, 40002, 40003. Équilibrage de charge de Web d'infrastructure vRealize Automation : 443 VMware ESXi : 902. Le Web d'infrastructure nécessite un accès au port 443 du point de terminaison VMware Remote Console pour obtenir un ticket pour vSphere. dispositif vRealize Automation nécessite un accès au port 902 de l'hôte ESXi pour transmettre via proxy les données de console à l'utilisateur. Authentification Kerberos : 88 Renouvellement du mot de passe de l'objet ordinateur : 464

Rôle de serveur	Ports entrants	Ports sortants pour service ou système
Serveur Web d'infrastructure	<p>HTTPS : 443</p> <p>MSDTC : 443, 1024-65535.</p> <p>Pour savoir comment mieux cibler cette plage, reportez-vous à la section de déploiement de la base de données de Déploiement de vRealize Automation.</p>	<p>Équilibrage de charge du dispositif vRealize Automation : 443</p> <p>Équilibrage de charge du dispositif vRealize Automation : 5480.</p> <p>Point de terminaison vSphere : 443. Le Web d'infrastructure nécessite un accès au port 443 du point de terminaison VMware Remote Console pour obtenir un ticket pour vSphere. Le dispositif vRealize Automation nécessite un accès au port 902 de l'hôte ESXi pour transmettre via proxy les données de console à l'utilisateur.</p> <p>MSSQL : 135, 1433, 1024 à 65535.</p> <p>Pour savoir comment mieux cibler cette plage, reportez-vous à la section de déploiement de la base de données de Déploiement de vRealize Automation.</p>
Serveur de gestionnaire d'infrastructure	<p>HTTPS : 443</p> <p>MSDTC : 135,1024-65535.</p> <p>Pour savoir comment mieux cibler cette plage, reportez-vous à la section de déploiement de la base de données de Déploiement de vRealize Automation.</p>	<p>Équilibrage de charge du dispositif vRealize Automation : 443</p> <p>Équilibrage de charge de Web d'infrastructure vRealize Automation : 443</p> <p>Dispositif vRealize Automation : 443, 5480</p> <p>MSSQL : 135, 1433, 1024 à 65535.</p> <p>Pour savoir comment mieux cibler cette plage, reportez-vous à la section de déploiement de la base de données de Déploiement de vRealize Automation.</p>
Serveur DEM d'infrastructure	SO	<p>Équilibrage de charge du dispositif vRealize Automation : 443</p> <p>Équilibrage de charge de Web d'infrastructure vRealize Automation : 443</p> <p>Équilibrage de charge de gestionnaire d'infrastructure vRealize Automation : 443</p> <p>Équilibrage de charge de vRealize Orchestrator : 8281</p> <p>Dispositif vRealize Automation : 5480.</p>

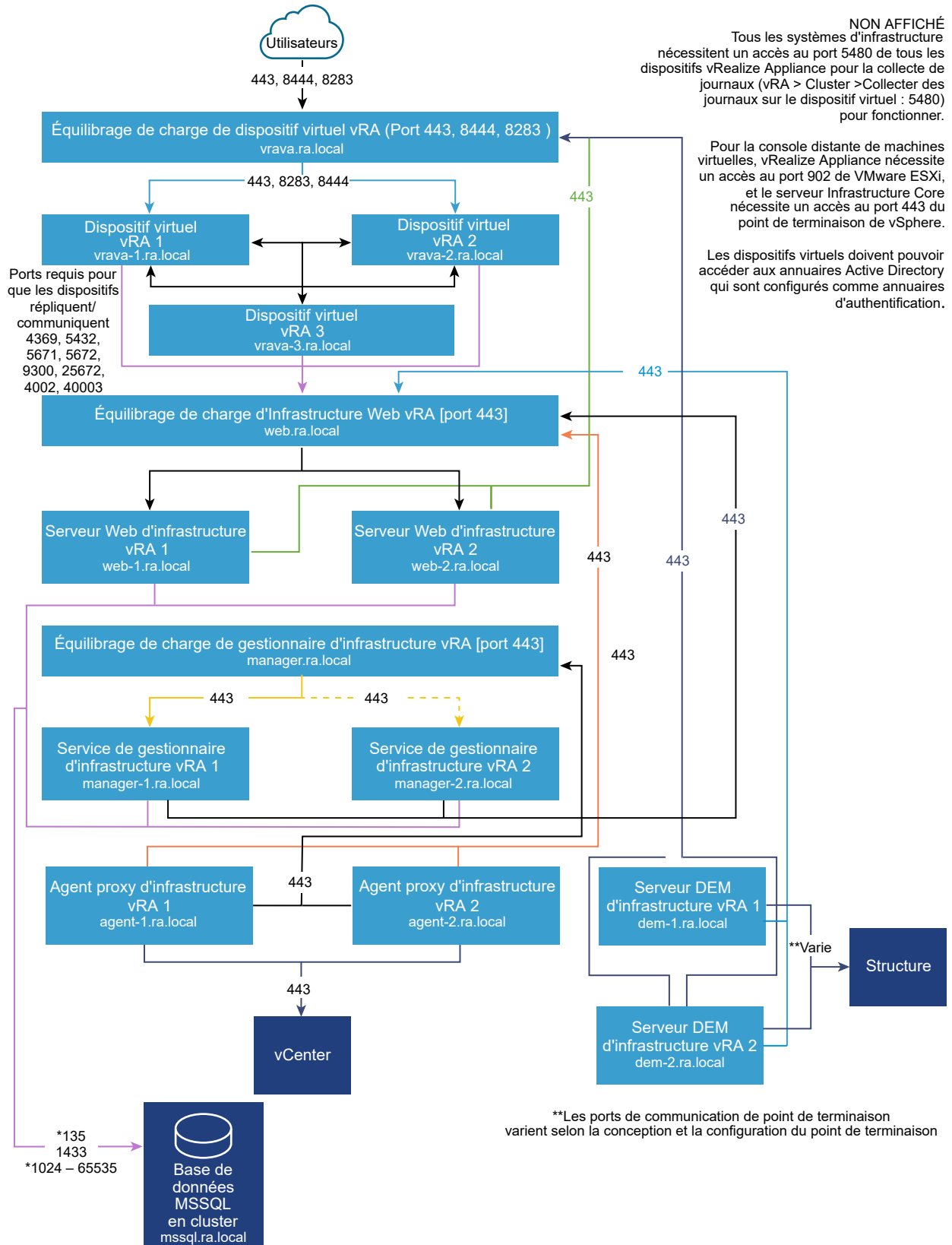
Rôle de serveur	Ports entrants	Ports sortants pour service ou système
Serveur d'agent d'infrastructure	SO	Équilibrage de charge de Web d'infrastructure vRealize Automation : 443 Équilibrage de charge de gestionnaire d'infrastructure vRealize Automation : 443 Dispositif vRealize Automation : 5480.
Serveur de base de données MSSQL	MSSQL : 1433 MSDTC : 135, 1024-65535. Pour savoir comment mieux cibler cette plage, reportez-vous à la section de déploiement de la base de données de Déploiement de vRealize Automation .	Serveur Web d'infrastructure : 135, 1024-65535. Pour savoir comment mieux cibler cette plage, reportez-vous à la section de déploiement de la base de données de Déploiement de vRealize Automation . Serveur de gestionnaire d'infrastructure : 135, 1024-65535. Pour savoir comment mieux cibler cette plage, reportez-vous à la section de déploiement de la base de données de Déploiement de vRealize Automation .
Serveur vRealize Business for Cloud	HTTPS : 443 SSH : 22 Interface de gestion du dispositif vRealize Automation : 5480	Équilibrage de charge du dispositif vRealize Automation : 443 Équilibrage de charge de Web d'infrastructure vRealize Automation : 443
Catalogue global		Catalogue global : 3268, 3269

Les équilibres de charge nécessitent un accès par les ports suivants.

Équilibrage de charge	Ports équilibrés
Équilibrage de charge du dispositif vRealize Automation	443, 8444
Équilibrage de charge de Web d'infrastructure vRealize Automation	443
Équilibrage de charge du serveur du gestionnaire vRealize Automation	443

Graphiques

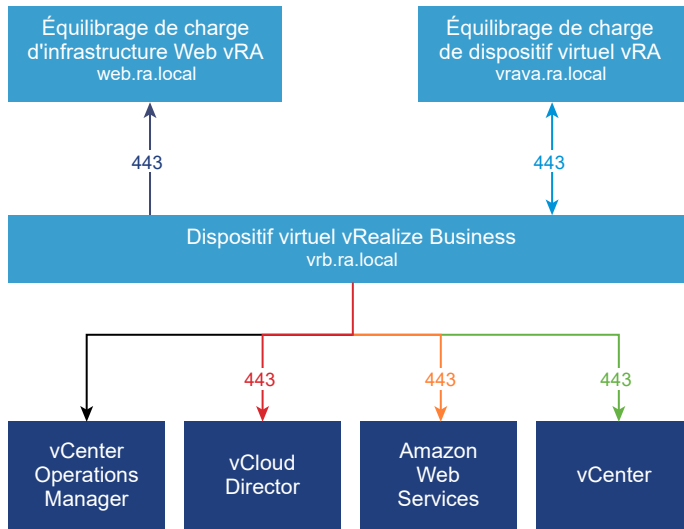
Figure 1-7. Encombrement minimal d'une grande configuration de vRealize Automation



*Reportez-vous à la section Déploiement de base de données pour découvrir comment mieux cibler cette page

En outre, une communication bidirectionnelle est requise.

Figure 1-8. Encombrement minimal d'une grande configuration de vRealize Business for Cloud



Déploiements de données de centre de données multiples dans vRealize Automation

vRealize Automation prend en charge la gestion des ressources dans des centres de données à distance.

Pour gérer les ressources vSphere, HyperV ou Xen dans des centres de données à distance, déployez l'agent proxy sur une machine virtuelle dans le centre de données distant.

Note Le diagramme ci-dessous présente un déploiement de vSphere. Les autres points de terminaison ne nécessitent aucune configuration supplémentaire.

Étant donné que les workflows de vRealize Orchestrator pourront potentiellement communiquer sur un réseau WAN, suivez les recommandations indiquées dans le *Guide de conception de codage de vRealize Orchestrator*.

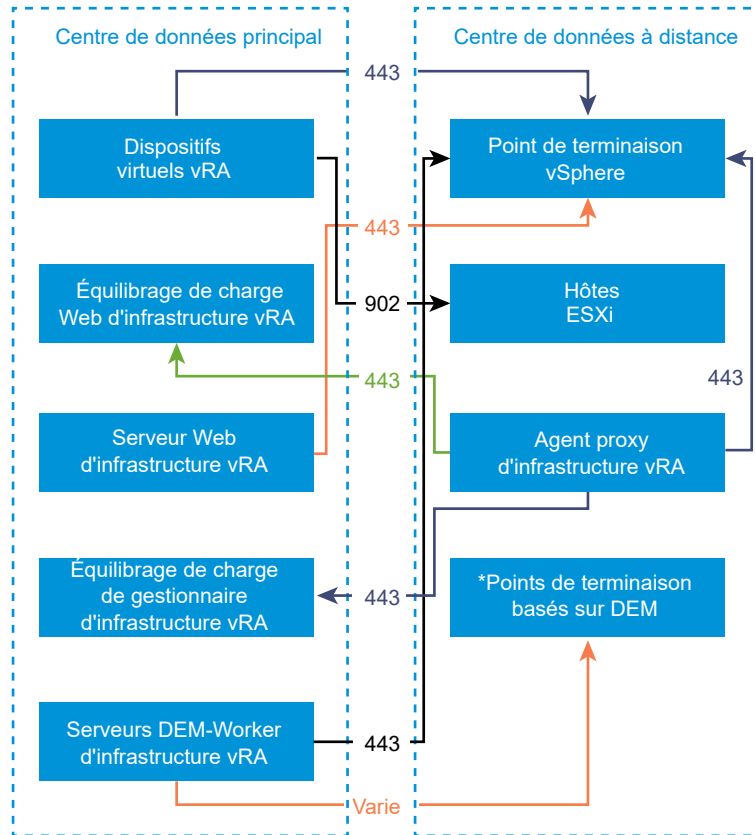
Tableau 1-10. Ports requis pour la communication WAN

Rôle	Ports entrants	Ports sortants des services/système
dispositif vRealize Automation - incluant vRealize Orchestrator intégré	S/O	Point de terminaison vSphere : 443 Hôtes ESXi : 902
Équilibreurs de charge d'infrastructure de vRealize Automation	Agent proxy d'infrastructure de vRealize Automation : 443	S/O
Infrastructure Web Server de vRealize Automation	S/O	Point de terminaison vSphere : 443
Équilibreurs de charge de gestionnaire d'infrastructure vRealize Automation	Agent proxy d'infrastructure de vRealize Automation : 443	S/O
Serveurs d'infrastructure DEM-worker de vRealize Automation	S/O	Point de terminaison : ** varie

* Si des DEM-workers sont installés sur la machine Manager Service ou sur un autre serveur, ces ports doivent être ouverts entre cette machine et le point de terminaison cible.

** Le port requis pour un communiquer avec un point de terminaison externe varie selon le point de terminaison. Par défaut, pour vSphere, il s'agit du port 443.

Figure 1-9. Configuration de sites multiples dans vRealize Automation



Installation de vRealize Automation

Suivez les instructions fournies pour installer une nouvelle instance de vRealize Automation.

Présentation de l'installation de vRealize Automation

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

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

À propos de l'installation de vRealize Automation

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

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

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

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

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

Nouveautés dans cette installation vRealize Automation

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

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

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

Composants d'installation de vRealize Automation

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

Le dispositif vRealize Automation

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

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

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

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

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

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

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

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

aaS (Infrastructure en tant que service)

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

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

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

Serveur Web

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

Model Manager

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

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

Manager Service

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

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

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

Base de données SQL Server

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

Distributed Execution Manager

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

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

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

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

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

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

Agents

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

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

Agents proxy de virtualisation

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

Un agent proxy de virtualisation a les caractéristiques suivantes.

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

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

Agents Virtual Desktop Integration (VDI)

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

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

Agents External Provisioning Integration (EPI)

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

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

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

Agent Windows Management Instrumentation

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

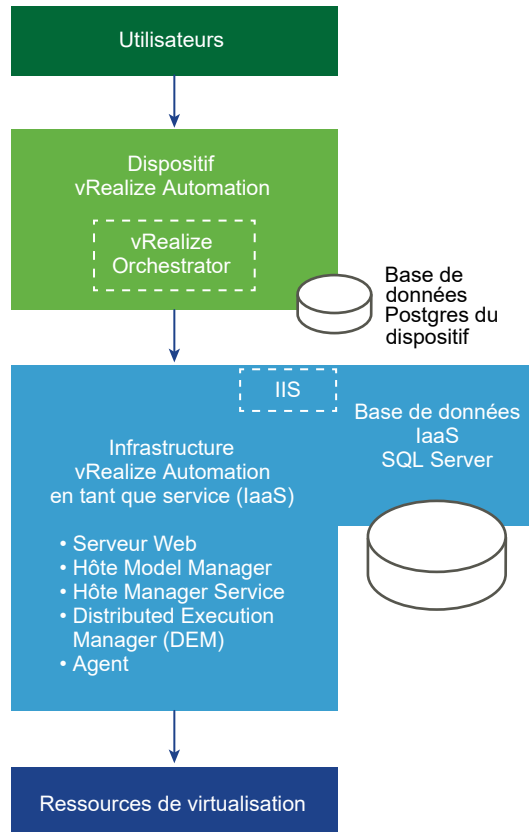
Type de déploiement

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

Déploiements vRealize Automation minimaux

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

Figure 1-10. Déploiement vRealize Automation minimal

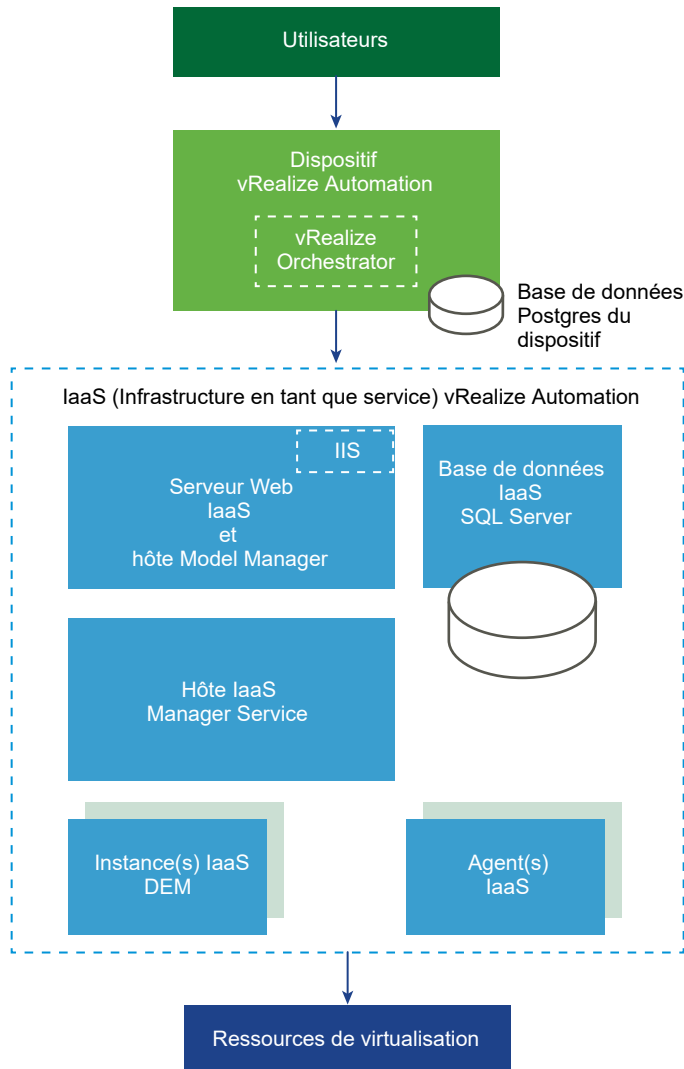


Vous ne pouvez pas convertir un déploiement minimal en un déploiement d'entreprise. Pour monter un déploiement en puissance, commencez par un déploiement de petite entreprise, puis ajoutez-y des composants. Il n'est pas possible de commencer avec un déploiement minimal.

Déploiements vRealize Automation distribués

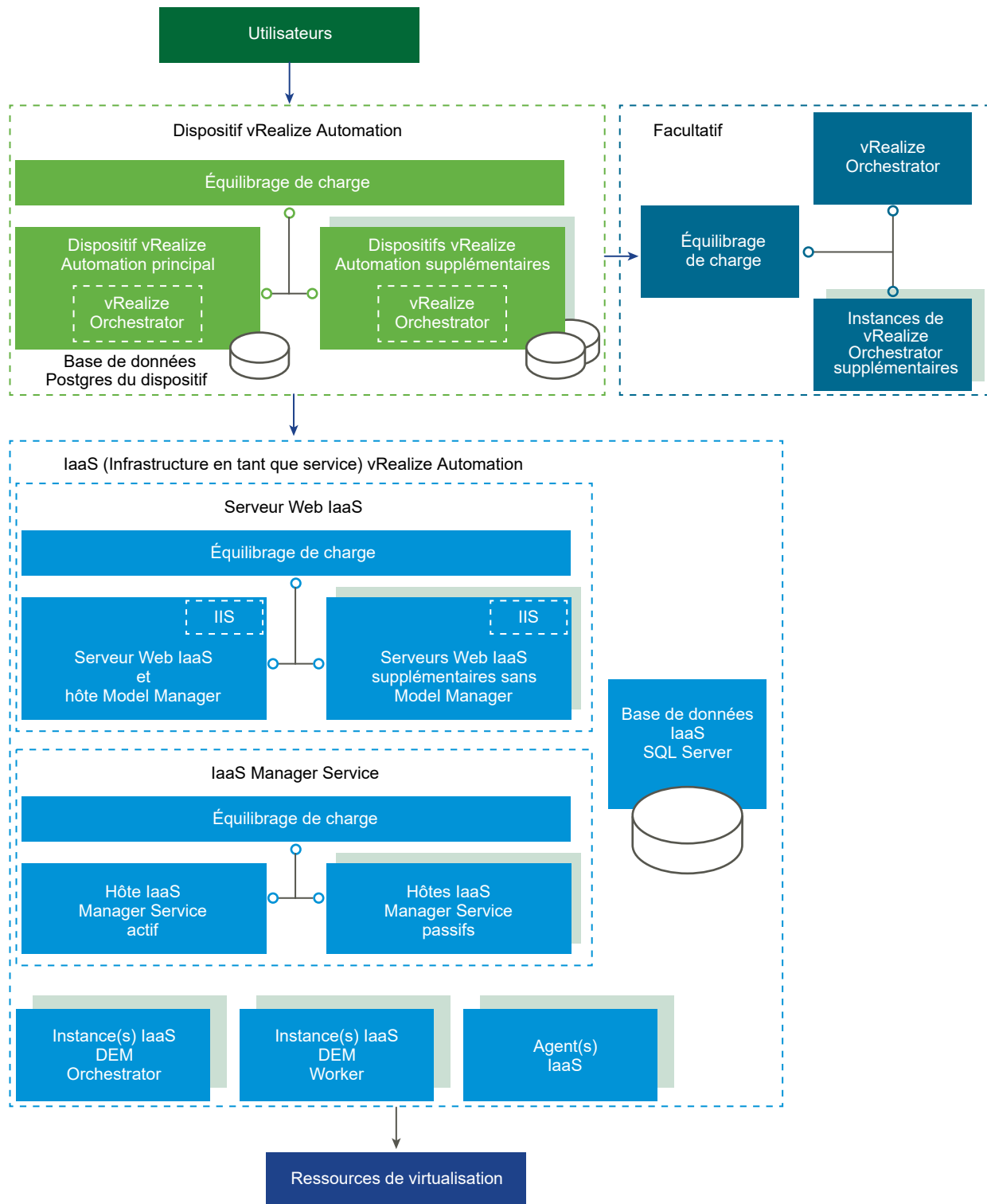
Les déploiements distribués d'entreprise peuvent avoir des tailles variables. Un déploiement distribué de base peut améliorer vRealize Automation simplement en hébergeant les composants IaaS sur des serveurs Windows distincts comme le montre la figure suivante.

Figure 1-11. Déploiement vRealize Automation distribué



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

Figure 1-12. Déploiement vRealize Automation distribué et faisant l'objet d'un équilibrage de charge



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

Choisir votre méthode d'installation

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

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

Préparation à l'installation de vRealize Automation

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

Préparation générale

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

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

Navigateurs Web utilisateur

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

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

Logiciels tiers

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

Synchronisation de l'heure

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

- L'hôte du dispositif vRealize Automation

- Un serveur NTP (Network Time Protocol) externe

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

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

Comptes et mots de passe

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

Compte de service laaS

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

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

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

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

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

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

- Accéder à cet ordinateur à partir du réseau—Ajouter le compte.

Identité de pool d'applications IIS

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

Informations d'identification de base de données IaaS

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

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

Phrase secrète de sécurité de la base de données IaaS

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

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

Points de terminaison vSphere

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

Mot de passe d'administrateur de vRealize Automation

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

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

Noms d'hôtes et adresses IP

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

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

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

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

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

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

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

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

- Pour les serveurs IaaS Windows, vous suivez le processus habituel du système d'exploitation. Définissez l'adresse IP avant d'installer vRealize Automation IaaS.

Latence et bande passante

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

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

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

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

- DEM Worker IaaS

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

- Agent proxy IaaS

Dispositif vRealize Automation

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

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

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

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

Tableau 1-11. Conditions matérielles requises du dispositif vRealize Automation pour Active Directory

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

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

Ports du dispositif vRealize Automation

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

Les ports suivants sont utilisés par le dispositif vRealize Automation.

Tableau 1-12. Ports entrants

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

Tableau 1-12. Ports entrants (suite)

Port	Protocole	Commentaires
54328	UDP	
40002, 40003	TCP	synchronisation du cluster vIDM
8090, 8092	TCP	Utilisé par le service de santé pour se connecter entre les nœuds vRA

Tableau 1-13. Ports sortants

Port	Protocole	Commentaires
25, 587	TCP, UDP	SMTP pour l'envoi d'un e-mail de notification sortant.
53	TCP, UDP	Serveur DNS.
67, 68, 546, 547	TCP, UDP	DHCP.
80	TCP	Facultatif. Pour extraire des mises à jour logicielles. Les mises à jour peuvent être téléchargées séparément et appliquées.
88, 464, 135	TCP, UDP	Contrôleur de domaine.
110, 995	TCP, UDP	POP pour recevoir un e-mail de notification entrant.
143, 993	TCP, UDP	IMAP pour recevoir un e-mail de notification entrant.
123	TCP, UDP	Facultatif. Pour la connexion directe au NTP au lieu d'utiliser l'heure de l'hôte.
389	TCP	Accès au serveur de connexion View.
389, 636, 3268, 3269	TCP	Active Directory. Les ports par défaut sont affichés, mais configurables.
443	TCP	Communication avec IaaS Manager Service et les hôtes des points de terminaison de l'infrastructure sur HTTPS.
		Communication avec le service de logiciel vRealize Automation sur HTTPS.
		Accès au serveur de mise à niveau Identity Manager.
		Accès au serveur de connexion View.
445	TCP	Accès au référentiel ThinApp pour Identity Manager.
902	TCP	Opérations de copie de fichiers réseau ESXi et connexions de VMware Remote Console.
5050	TCP	Facultatif. Pour communiquer avec vRealize Business for Cloud.
5432	TCP, UDP	Facultatif. Pour communiquer avec une autre base de données PostgreSQL du dispositif.
5500	TCP	Système RSA SecurID. Le port par défaut est affiché, mais configurable.
8281	TCP	Facultatif. Pour communiquer avec une instance de vRealize Orchestrator externe.

Tableau 1-13. Ports sortants (suite)

Port	Protocole	Commentaires
8494	TCP	Synchronisation du cluster de service de conteneur
9300–9400	TCP	Accès pour les audits Identity Manager.
54328	UDP	
40002, 40003	TCP	synchronisation du cluster vIDM

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

Serveurs Windows IaaS

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

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

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

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

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

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

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

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

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

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

- Pour tout déploiement d'une taille supérieure à la valeur minimale, définissez Serveurs Windows IaaS sur les paramètres régionaux anglais.
- Si vous installez plusieurs composants IaaS sur le même serveur Windows, prévoyez de les installer dans le même dossier d'installation. N'utilisez pas des chemins d'accès distincts.
- Les serveurs IaaS utilisent TLS à des fins d'authentification, une option activée par défaut sur certains serveurs Windows.

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

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

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

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

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

Ports de serveur Windows IaaS

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

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

Tableau 1-14. Ports entrants

Port	Protocole	Composant	Commentaires
443	TCP	Manager Service	Communication avec les composants IaaS et le dispositif vRealize Automation sur HTTPS.
443	TCP	Dispositif vRealize Automation	Communication avec les composants IaaS et le dispositif vRealize Automation sur HTTPS.
443	TCP	Hôtes des points de terminaison de l'infrastructure	Communication avec les composants IaaS et le dispositif vRealize Automation sur HTTPS. En général, le port 443 est le port de communication par défaut des hôtes des points de terminaison de l'infrastructure virtuelle et de cloud, mais reportez-vous à la documentation fournie par vos hôtes d'infrastructure pour obtenir la liste complète des ports par défaut et des ports requis
443	TCP	Agent invité agent de démarrage logiciel	Communication avec Manager Service sur HTTPS
443	TCP	DEM Worker	Communication avec NSX Manager
1433	TCP	Instance du serveur SQL Server	MSSQL

Tableau 1-15. Ports sortants

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

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

Serveur Web IaaS

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

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

- Configurez Java.
 - Installez Java 64 bits 1.8, mise à jour 191. N'utilisez pas la version 32 bits.
JRE est suffisant. Vous n'avez pas besoin du JDK complet.
 - Définissez la variable d'environnement JAVA_HOME sur le dossier d'installation de Java.
 - Vérifiez que le fichier %JAVA_HOME%\bin\java.exe est disponible.
- Configurez IIS (Internet Information Services) en fonction du tableau suivant.
Vous avez besoin d'IIS 7.5 pour les variantes de Windows 2008, d'IIS 8 pour Windows 2012, d'IIS 8.5 pour Windows 2012 R2 et d'IIS 10 pour Windows 2016.

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

Tableau 1-16. IaaS Internet Information Services

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

Hôte Manager Service IaaS

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

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

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

Hôte du serveur SQL IaaS

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

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

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

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

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

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

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

Hôte DEM (Distributed Execution Manager) IaaS

Un serveur Windows qui héberge le composant DEM (Distributed Execution Manager) Orchestrator ou Worker doit répondre aux conditions requises supplémentaires, en plus de celles de tous les serveurs Windows IaaS.

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

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

DEM Workers avec Amazon Web Services

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

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

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

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

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

DEM Workers avec Openstack ou PowerVC

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

Tableau 1-17. Configuration requise des DEM Workers Openstack et PowerVC

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

DEM Workers avec virtualisation Red Hat

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

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

DEM Workers avec SCVMM

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

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

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

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

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

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

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

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

Les conditions requises supplémentaires suivantes s'appliquent à SCVMM.

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

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

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

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

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

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

- Pour provisionner des machines sur une ressource SCVMM, l'utilisateur vRealize Automation qui demande l'article du catalogue doit avoir le rôle d'administrateur dans l'instance de SCVMM.

- Les serveurs Hyper-V situés dans une instance de SCVMM é gérer doivent être des serveurs Windows 2008 R2 SP1 sur lesquels Hyper-V est installé. Le processeur doit être équipé des extensions de virtualisation requises .NET Framework 4.5.2 ou version ultérieure doit être installé et Windows Management Instrumentation (WMI) doit être activé.
- Pour provisionner une machine Generation-2 sur une ressource SCVMM 2012 R2, vous devez ajouter les propriétés suivantes au Blueprint.

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

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

Pour plus d'informations sur la préparation du provisionnement de machine, reportez-vous à la section [Préparation de votre environnement SCVMM](#).

Certificats

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

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

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

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

Tableau 1-18. Mise en œuvre des certificats

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

Chaînes de certificats

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

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

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

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

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

Exigences en matière de certificats vRealize Automation

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

Types de certificats pris en charge

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

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

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

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

Matrice de prise en charge de certificats vRealize Automation

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

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

Extraction de certificats et de clés privées

Les certificats des dispositifs virtuels doivent être au format PEM.

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

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


Par exemple :

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

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

Déploiement du dispositif vRealize Automation

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

À propos du déploiement du dispositif vRealize Automation

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

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

Déployer le dispositif vRealize Automation

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

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

Conditions préalables

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

Procédure

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

5 Entrez un nom de dispositif et un emplacement d'inventaire.

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

6 Sélectionnez l'hôte et le cluster dans lesquels le dispositif va résider.

7 Sélectionnez le pool de ressources dans lequel le dispositif va résider.

8 Sélectionnez le stockage qui hébergera le dispositif.

9 Sélectionnez un format de disque.

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

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

10 Dans le menu déroulant, sélectionnez un réseau de Destination.

11 Terminez les propriétés du dispositif.

a Entrez et confirmez un mot de passe racine.

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

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

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

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

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

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

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

Figure 1-13. Exemple de propriétés de dispositif virtuel

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

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

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

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

Étape suivante

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

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

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

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

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

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

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

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

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

Conditions préalables

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

Procédure

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

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

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

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

Par exemple :

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

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

Étape suivante

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

Installation de vRealize Automation avec l'assistant Installation

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

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

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

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

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

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

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

Démarrer l'assistant d'installation pour un déploiement minimal

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

Conditions préalables

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

Procédure

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

Étape suivante

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

Installer l'agent de gestion vRealize Automation

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

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

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

Conditions préalables

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

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

Procédure

1 Connectez-vous à la console du dispositif vRealize Automation en tant qu'utilisateur racine.

2 Entrez la commande suivante :

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

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

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

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

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

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

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

7 Lisez le message d'accueil.

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

9 Acceptez ou modifiez le dossier d'installation.

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


10 Entrez les détails du dispositif vRealize Automation :

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

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

Figure 1-14. Agent de gestion - Détails du dispositif vRealize Automation

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

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

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

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

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

Étape suivante

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

Exécution de l'assistant d'installation

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

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

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

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

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

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

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

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

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

Conditions préalables

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

Procédure

- 1 Connectez-vous à l'interface d'administration du dispositif vRealize Automation en tant qu'utilisateur racine.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Lorsque l'assistant d'installation s'affiche, cliquez sur **Suivant**.
- 3 Acceptez le contrat de licence d'utilisateur final, puis cliquez sur **Suivant**.

- 4 Sur la page Type de déploiement, sélectionnez **Déploiement d'entreprise** et **Installer les infrastructures en tant que service**.
- 5 Sur la page Conditions préalables d'installation, connectez-vous aux serveurs IaaS Windows et installez l'agent de gestion. L'agent de gestion permet au dispositif vRealize Automation de détecter ces serveurs IaaS et de s'y connecter.

Étape suivante

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

Installer l'agent de gestion vRealize Automation

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

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

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

Conditions préalables

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

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

Procédure

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

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

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

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

- 6 Cliquez sur **Programme d'installation de l'agent de gestion**, puis enregistrez et exécutez le fichier .msi.
- 7 Lisez le message d'accueil.
- 8 Acceptez l'accord de licence d'utilisateur final.
- 9 Acceptez ou modifiez le dossier d'installation.
Program Files (x86)\VMware\VCAC\Management Agent
- 10 Entrez les détails du dispositif vRealize Automation principal :
 - a Entrez l'adresse HTTPS du dispositif principal, y compris le nom de domaine complet et le numéro de port 5480.
 - b Entrez les informations d'identification du compte racine du dispositif principal.
 - c Cliquez sur **Charger** et assurez-vous que l'empreinte digitale correspond à celle précédemment copiée. Ignorez les deux-points.

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

Figure 1-15. Agent de gestion - Détails du dispositif vRealize Automation

- 11 Entrez le domaine\nom d'utilisateur et le mot de passe du compte de service.
Le compte de service doit être un compte de domaine disposant des droits d'administrateur sur les serveurs Windows IaaS. Utilisez partout le même compte de service.
- 12 Suivez les invites pour terminer l'installation de l'agent de gestion.

Résultats

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

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

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

Étape suivante

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

Exécution de l'assistant d'installation

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

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

Suivre les étapes de l'assistant d'installation de vRealize Automation

L'assistant d'installation de vRealize Automation vous présente des pages faciles à utiliser sur lesquelles vous pouvez vérifier des conditions préalables, entrer des paramètres, valider des paramètres et installer des composants vRealize Automation.

Note L'assistant inclut des étapes au cours desquelles vous vous connectez à d'autres systèmes tels que des équilibres de charge et des serveurs Windows IaaS.

Conditions préalables

- Créez un ou plusieurs dispositifs non configurés. Reportez-vous à [Déployer le dispositif vRealize Automation](#).

Les déploiements minimaux utilisent un dispositif vRealize Automation. Les déploiements d'entreprise peuvent avoir plusieurs dispositifs derrière l'équilibre de charge.
- Veillez à avoir un ou plusieurs systèmes Windows disponibles sur lesquels héberger des composants IaaS.
- Démarrez l'assistant en vous connectant à l'interface d'administration du dispositif vRealize Automation en tant qu'utilisateur racine.

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

Procédure

1 Type de déploiement

Sur la page Type de déploiement, vous décidez les composants vRealize Automation que vous souhaitez installer et leur nombre.

2 Conditions préalables d'installation

Sur la page Conditions préalables d'installation, vous pouvez établir une connexion aux machines Windows qui hébergeront vRealize AutomationlaaS. En outre, vous sélectionnez une source de synchronisation de l'heure.

3 vRealize Appliances

(Déploiements d'entreprise uniquement) Sur la page de vRealize Appliances, vous avez la possibilité de créer un déploiement à haute disponibilité avec plusieurs dispositifs vRealize Automation.

4 Rôles de serveur

(Déploiements d'entreprise uniquement) Sur la page Rôles de serveur, vous attribuez des rôles de composant vRealize AutomationlaaS aux machines Windows sur lesquelles vous avez installé l'agent de gestion précédemment.

5 Outil de vérification des conditions préalables

Sur la page Programme de vérification des conditions préalables, vérifiez et corrigez vos serveurs Windows vRealize Automation pour prendre en charge l'installation laaS.

6 Hôte vRealize Automation

Sur la page Hôte vRealize Automation, vous définissez l'adresse URL de base pour vRealize Automation. L'adresse est généralement le dispositif vRealize Automation ou, dans les déploiements à haute disponibilité, un équilibrage de charge.

7 Single Sign-On

Sur la page Single Sign-On, vous définissez les informations d'identification de connexion de l'administrateur système locataire vRealize Automation par défaut.

8 Hôte laaS

Sur la page Hôte laaS, définissez les adresses URL de base pour certains composants laaS. Créez également une phrase secrète de sécurité pour la base de données SQL laaSvRealize Automation.

9 Microsoft SQL Server

Sur la page Microsoft SQL Server, vous configurez la base de données SQL vRealize AutomationlaaS. La base de données laaS enregistre les machines provisionnées, les éléments associés et les stratégies.

10 Rôle Web

(Déploiements d'entreprise uniquement) Sur la page Rôle Web, vous configurez séparément le site Web de vRealize AutomationIaaS dans IIS.

11 Rôle du service de gestionnaire

(Déploiements d'entreprise uniquement) Sur la page Rôle du service de gestionnaire, vous configurez la machine Windows vRealize Automation distincte qui héberge le service de gestionnaire IaaS .

12 Instances de Distributed Execution Manager

Sur la page Instances de Distributed Execution Manager, vous configurez les machines Windows vRealize Automation qui hébergent des composants DEM IaaS. Plusieurs hôtes DEM sont pris en charge.

13 Agents

Sur la page Agents, vous créez la liaison entre vRealize AutomationIaaS et les ressources de virtualisation sur lesquelles l'infrastructure est déployée. Vous sélectionnez un type d'agent et indiquez les détails du point de terminaison correspondant.

14 Certificat vRealize Appliance

Sur la page Certificat vRealize Appliance, vous créez ou sélectionnez le certificat d'authentification utilisé par le dispositif vRealize Automation. Lorsque le certificat est autosigné, les utilisateurs finaux peuvent le voir et le confirmer lorsqu'ils se connectent à vRealize Automation dans un navigateur.

15 Certificat Web

Sur la page Certificat Web, vous créez ou sélectionnez le certificat d'authentification utilisé par le serveur Web IaaS. Le dispositif vRealize Automation se connecte au serveur Web et doit s'y authentifier et l'approuver.

16 Certificat du service de gestionnaire

(Déploiements d'entreprise uniquement) Sur la page Certificat du service de gestionnaire, vous créez ou sélectionnez le certificat d'authentification utilisé par l'hôte du service de gestionnaire vRealize AutomationIaaS. Les autres serveurs Windows IaaS se connectent à l'hôte du service de gestionnaire et doivent s'y authentifier et l'approuver.

17 Équilibrages de charge

(Déploiements d'entreprise uniquement) Sur la page Équilibrages de charge, prenez le temps de configurer les équilibrages de charge du pool correct des systèmes membres de vRealize Automation.

18 Validation

Sur la page Validation, vérifiez que l'installation de vRealize Automation peut continuer.

19 Créer des snapshots

Sur la page Créer des snapshots, vous pouvez prendre des snapshots de machine virtuelle de tous les composants vRealize Automation avant de poursuivre l'installation.

20 Détails de l'installation

Sur la page Détails de l'installation, vous démarrez l'installation de vRealize Automation ou effectuez une nouvelle tentative si des problèmes sont survenus.

21 Attribution de licence

Sur la page Attribution de licence, vous entrez une clé pour activer le produit vRealize Automation installé.

22 Télémétrie

Sur la page Télémétrie, vous décidez si vRealize Automation peut envoyer ou non des statistiques d'utilisation à VMware dans le cadre du Programme d'amélioration du produit.

23 Options après installation

Sur la page Options après installation, vous disposez d'options de création de données vRealize Automation ou de migration des anciennes données de déploiement vers votre nouvelle installation.

24 Configuration du contenu initial

Sur la page Configuration du contenu initial, vous créez un nouvel utilisateur locataire par défaut vRealize Automation local qui peut commencer un workflow de contenu pour un point de terminaison vSphere.

25 Configuration de la migration

Sur la page Configuration de la migration, vous pouvez démarrer le transfert d'un ancien déploiement vRealize Automation vers le déploiement que vous venez d'installer.

Type de déploiement

Sur la page Type de déploiement, vous décidez les composants vRealize Automation que vous souhaitez installer et leur nombre.

Minimal

Les déploiements minimaux utilisent seulement un dispositif vRealize Automation et un serveur Windows qui héberge les composants IaaS. Dans les déploiements minimaux, vous pouvez héberger la base de données IaaS sur un système SQL Server distinct ou installer SQL sur le serveur Windows IaaS.

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

Entreprise

Les déploiements d'entreprise impliquent plusieurs hôtes Windows et dispositifs distincts, généralement avec équilibrage de charge. Les déploiements d'entreprise vous permettent également d'héberger la base de données IaaS sur un système SQL Server distinct ou sur l'un des serveurs Windows IaaS.

Lorsque vous sélectionnez un déploiement d'entreprise, les autres pages de l'assistant d'installation apparaissent dans la liste récapitulative à gauche de l'assistant.

IaaS (Infrastructure en tant que service)

L'option IaaS (Infrastructure en tant que service) (IaaS) permet de choisir la configuration ou non des machines Windows existantes avec des capacités de provisionnement et de modélisation vRealize Automation.

Bien que la plupart des utilisateurs l'installent, vRealize Automation n'a pas strictement besoin de IaaS. Si vous n'avez besoin que de la prise en charge du provisionnement XaaS, vous pouvez installer uniquement le dispositif vRealize Automation. Dans cette configuration, un message d'avertissement s'affiche dans l'interface de gestion du dispositif vRealize Automation. Vous pouvez désactiver le message en modifiant `/etc/vcac/validation.properties`. Basculez `iaas.primary.web.validation.enabled` sur `False`.

Lorsque vous sélectionnez IaaS, les autres pages de l'assistant d'installation apparaissent dans la liste récapitulative à gauche de l'assistant.

Conditions préalables d'installation

Sur la page Conditions préalables d'installation, vous pouvez établir une connexion aux machines Windows qui hébergeront vRealize Automation IaaS. En outre, vous sélectionnez une source de synchronisation de l'heure.

Serveurs Windows IaaS

Pour une machine Windows destinée à servir d'hôte pour composants IaaS, vous devez télécharger et installer `VCAC-IaaSManagementAgent-Setup.msi` sur cette machine Windows.

L'installation de l'agent de gestion nécessite une communication avec un dispositif vRealize Automation en cours d'exécution. Chaque fois que vous installez l'agent de gestion sur Windows, ce système devient exclusivement lié au dispositif et au déploiement spécifiques.

Les serveurs Windows IaaS potentiels sur lesquels l'agent de gestion adapté est installé s'affichent sous **Hôtes découverts**.

Pour que l'assistant d'installation ignore un hôte découvert, cliquez sur **Supprimer**. La suppression d'un hôte Windows ne supprime pas son agent de gestion. Pour désinstaller l'agent, utilisez la fonction Ajouter ou supprimer des programmes directement dans Windows.

Source de temps

Vous devez synchroniser chaque dispositif vRealize Automation et serveur Windows IaaS avec la même source de temps. Les sources suivantes sont autorisées :

- Utiliser l'heure de l'hôte — Synchronisation avec l'hôte ESXi du dispositif vRealize Automation.
- Utiliser le serveur de temps — Synchronisation avec un serveur NTP (Network Time Protocol) externe. Entrez le nom de domaine complet ou l'adresse IP du serveur NTP.

Ne mélangez pas les sources de temps au sein d'un déploiement vRealize Automation .

vRealize Appliances

(Déploiements d'entreprise uniquement) Sur la page de vRealize Appliances, vous avez la possibilité de créer un déploiement à haute disponibilité avec plusieurs dispositifs vRealize Automation.

Plusieurs dispositifs doivent être hébergés derrière un équilibrage de charge que vous avez installé séparément. Sur une page d'assistant ultérieure, vous vérifiez et terminez la configuration des dispositifs et de l'équilibrage de charge. Pour chaque dispositif vRealize Automation ajouté, entrez son nom de domaine complet et ses informations d'identification racine.

Rôles de serveur

(Déploiements d'entreprise uniquement) Sur la page Rôles de serveur, vous attribuez des rôles de composant vRealize AutomationIaaS aux machines Windows sur lesquelles vous avez installé l'agent de gestion précédemment.

Les machines Windows IaaS peuvent servir de serveurs Web principaux et supplémentaires, d'hôtes Manager Service, d'hôtes DEM et d'hôtes d'agent. Pour en savoir plus sur les rôles de composant IaaS, reportez-vous à la section [IaaS \(Infrastructure en tant que service\)](#).

La séparation des rôles de serveur IaaS est uniquement possible dans les déploiements d'entreprise. Dans les déploiements minimaux, une machine Windows remplit tous les rôles.

Outil de vérification des conditions préalables

Sur la page Programme de vérification des conditions préalables, vérifiez et corrigez vos serveurs Windows vRealize Automation pour prendre en charge l'installation IaaS.

Le programme de vérification des conditions préalables inspecte les machines virtuelles Windows sur lequel vous avez installé l'agent de gestion et qui hébergeront les composants IaaS. Les conditions préalables incluent les paramètres Java, Internet Information Services (IIS), le service Distributed Transaction Coordinator (DTC) Microsoft et plus encore. Pour obtenir une liste détaillée des conditions préalables, cliquez sur **Afficher les détails**.

L'assistant d'installation vous permet de continuer sans la vérification des conditions préalables, mais sachez que l'installation peut échouer.

- Pour vérifier les conditions préalables, cliquez sur **Exécuter**.
- Si les conditions préalables sont manquantes, cliquez sur **Afficher les détails** pour en savoir plus, puis cliquez sur **Corriger**.

L'assistant d'installation peut corriger la plupart des conditions préalables logicielles ou basées sur des paramètres. Après avoir effectué les modifications, l'assistant d'installation redémarre vos hôtes IaaS.

L'assistant ne peut pas corriger des problèmes de quantité insuffisante de mémoire ou de CPU. Lorsqu'il s'en produit, vous devez corriger ces problèmes dans vSphere ou sur votre matériel.

Hôte vRealize Automation

Sur la page Hôte vRealize Automation, vous définissez l'adresse URL de base pour vRealize Automation. L'adresse est généralement le dispositif vRealize Automation ou, dans les déploiements à haute disponibilité, un équilibrage de charge.

- Lors du déploiement d'un unique dispositif vRealize Automation sans équilibrage de charge, entrez le nom de domaine complet du dispositif vRealize Automation. Vous pouvez cliquer pour que l'assistant d'installation renseigne automatiquement le nom de domaine complet.
- Lors du déploiement d'une configuration d'entreprise qui inclut un ou plusieurs dispositifs vRealize Automation derrière un équilibrage de charge, entrez alors le nom de domaine complet de l'équilibrage de charge.

Un dispositif vRealize Automation unique peut toujours être déployé derrière un équilibrage de charge. Cette méthode vous permet d'ajouter plus facilement des dispositifs supplémentaires, afin de développer le déploiement.

Single Sign-On

Sur la page Single Sign-On, vous définissez les informations d'identification de connexion de l'administrateur système locataire vRealize Automation par défaut.

L'administrateur système locataire par défaut a plus d'autorisations que n'importe quel utilisateur, y compris la création de locataires supplémentaires. Les informations d'identification de l'administrateur système locataire par défaut sont distinctes des informations d'identification racine du dispositif vRealize Automation.

Hôte IaaS

Sur la page Hôte IaaS, définissez les adresses URL de base pour certains composants IaaS. Créez également une phrase secrète de sécurité pour la base de données SQL IaaS vRealize Automation.

Déploiements minimaux

Configuration	Description
Adresse Web IaaS	Entrez le nom de domaine complet du serveur Windows IaaS.
Installez les composants IaaS sur	Sélectionnez ou entrez le nom de domaine complet du serveur Windows IaaS.
Nom d'utilisateur	Au format DOMAIN\username, entrez le compte de service. Le compte doit être un compte de domaine avec des privilèges d'administrateur local sur le serveur Windows IaaS.
Mot de passe	Entrez le mot de passe du compte.

Configuration	Description
Phrase secrète de sécurité	<p>Créer une phrase secrète pour chiffrer les données dans la base de données SQL IaaS.</p> <ul style="list-style-type: none"> ■ Enregistrez la phrase secrète, car vous en avez besoin pour restaurer la base de données en cas de panne ou pour ajouter des composants après l'installation initiale. ■ La phrase secrète ne peut pas contenir de guillemet double (").
Confirmer la phrase secrète	Entrez à nouveau la phrase secrète.

Déploiements d'entreprise

Configuration	Description
Adresse Web IaaS	Entrez le nom de domaine complet du serveur Web IaaS principal. Si le déploiement d'une configuration d'entreprise incluant plusieurs serveurs Web IaaS à équilibrage de charge, entrez le nom de domaine complet de l'équilibrage de charge à la place.
Adresse de Manager Service	Entrez le nom de domaine complet de l'hôte Manager Service principal. Si le déploiement d'une configuration d'entreprise incluant plusieurs hôtes Manager Service à équilibrage de charge, entrez le nom de domaine complet de l'équilibrage de charge à la place.
Phrase secrète de sécurité	<p>Créer une phrase secrète pour chiffrer les données dans la base de données SQL IaaS.</p> <ul style="list-style-type: none"> ■ Enregistrez la phrase secrète, car vous en avez besoin pour restaurer la base de données en cas de panne ou pour ajouter des composants après l'installation initiale. ■ La phrase secrète ne peut pas contenir de guillemet double (").
Confirmer la phrase secrète	Entrez à nouveau la phrase secrète.

Microsoft SQL Server

Sur la page Microsoft SQL Server, vous configurez la base de données SQL vRealize AutomationIaaS. La base de données IaaS enregistre les machines provisionnées, les éléments associés et les stratégies.

Configuration	Description
Nom du serveur	<p>Entrez le nom de domaine complet de l'hôte SQL Server, qui peut être un serveur Windows IaaS ou un serveur séparé.</p> <p>Si vous devez spécifier un numéro de port ou une instance nommée, utilisez le format <code>Nom de domaine complet,Port\Instance</code>.</p> <p>Lorsque vous utilisez la fonctionnalité Groupe de disponibilité AlwaysOn (AAG), vous spécifiez le nom de domaine complet de l'écouteur AAG.</p>
Nom de la base de données	Acceptez la valeur par défaut vra ou entrez un nom différent pour la base de données IaaS.
Créer une base de données	<p>Autorisez l'Assistant d'installation à créer la base de données.</p> <p>Pour que cette option fonctionne, le compte qui exécute l'agent de gestion sur le serveur Web IaaS principal doit avoir le rôle sysadmin dans SQL.</p>

Configuration	Description
Utiliser une base de données vide existante	N'autorisez pas l'Assistant d'installation à créer la base de données. Lorsque vous créez la base de données séparément, les informations d'identification de l'utilisateur Windows ou de l'utilisateur SQL que vous fournissez doivent avoir l'autorisation dbo sur la base de données.
Paramètres par défaut	(Nouvelle base de données uniquement) Désactivez cette option uniquement si vous souhaitez utiliser un emplacement de stockage alternatif pour les données IaaS et les fichiers journaux. Lorsqu'elle est désactivée, entrez les répertoires des données (MDF) et des journaux. Votre compte de service SQL Server doit avoir l'autorisation d'écriture pour ces répertoires.
Utiliser SSL pour la connexion à la base de données	Chiffrez les connexions à la base de données. Pour utiliser cette option, vous devez configurer séparément votre hôte SQL Server pour SSL. En outre, le serveur Web IaaS et l'hôte Manager Service doivent approuver le certificat SSL à partir de votre hôte SQL Server.
Authentification Windows	Désactivez cette option uniquement si vous souhaitez utiliser l'authentification SQL au lieu de Windows. Lorsqu'elle est désactivée, entrez les informations d'identification de l'authentification SQL.
Chemin d'installation	Gardez cette option désactivée pour accepter la valeur par défaut %ProgramFiles(x86)%\VMware ou entrez un autre emplacement. <ul style="list-style-type: none"> ■ Les fichiers vRealize Automation ne sont pas installés sur l'hôte SQL Server. Ils sont placés sur le serveur Web IaaS principal. ■ Si vous installez plusieurs composants IaaS sur la même machine Windows, installez-les sous le même chemin d'installation.

Rôle Web

(Déploiements d'entreprise uniquement) Sur la page Rôle Web, vous configurez séparément le site Web de vRealize Automation IaaS dans IIS.

Dans un déploiement d'entreprise, vous spécifiez séparément la machine Windows IaaS qui héberge le composant Web. Pour la haute disponibilité, plusieurs hôtes sont pris en charge.

Configuration	Description
Nom du site Web	Personnalisez le nom ou laissez le site Web IIS par défaut. Évitez d'héberger des sites Web supplémentaires dans IIS. vRealize Automation définit la liaison sur son port de communication sur toutes les adresses IP non attribuées, ce qui ne permet aucune autre liaison.
Port	Personnalisez le port ou acceptez la valeur par défaut 443.
Serveurs Web IaaS	Nom d'hôte IaaS Entrez le nom de domaine complet de chaque machine Windows IaaS qui héberge le composant Web IaaS.
	Nom d'utilisateur Au format DOMAIN\username, entrez le compte de service. Le compte doit être un compte de domaine avec des privilèges d'administrateur local sur le serveur Windows IaaS.

Configuration	Description
Mot de passe	Entrez le mot de passe du compte.
Chemin d'installation	<p>Gardez cette option désactivée pour accepter la valeur par défaut %ProgramFiles(x86)%\VMware ou entrez un autre emplacement.</p> <p>Si vous installez plusieurs composants IaaS sur la même machine Windows, installez-les sous le même chemin d'installation.</p>

Rôle du service de gestionnaire

(Déploiements d'entreprise uniquement) Sur la page Rôle du service de gestionnaire, vous configurez la machine Windows vRealize Automation distincte qui héberge le service de gestionnaire IaaS .

Dans un déploiement d'entreprise, vous spécifiez séparément l'hôte du service de gestionnaire, qui est un service Windows. Pour la haute disponibilité, plusieurs hôtes sont pris en charge.

Configuration	Description
Actif	<p>Sélectionnez l'hôte du service de gestionnaire principal. Tous les hôtes supplémentaires servent de sauvegardes à l'instance principale.</p> <p>Lorsque vous effectuez l'installation à l'aide de l'assistant d'installation, le service bascule de manière transparente vers une sauvegarde lorsqu'un problème survient. Reportez-vous à À propos du basculement automatique de Manager Service .</p>
Nom d'hôte IaaS	Entrez le nom de domaine complet de chaque machine Windows IaaS qui héberge le service de gestionnaire.
Nom d'utilisateur	Au format DOMAIN\username, entrez le compte de service. Le compte doit être un compte de domaine avec des privilèges d'administrateur local sur le serveur Windows IaaS.
Mot de passe	Entrez le mot de passe du compte.
Chemin d'installation	<p>Gardez cette option désactivée pour accepter la valeur par défaut %ProgramFiles(x86)%\VMware ou entrez un autre emplacement.</p> <p>Si vous installez plusieurs composants IaaS sur la même machine Windows, installez-les sous le même chemin d'installation.</p>

Instances de Distributed Execution Manager

Sur la page Instances de Distributed Execution Manager, vous configurez les machines Windows vRealize Automation qui hébergent des composants DEM IaaS. Plusieurs hôtes DEM sont pris en charge.

Configuration	Description
Nom d'hôte laaS	Entrez le nom de domaine complet de chaque machine Windows laaS qui héberge un DEM.
Nom de l'instance	Entrez un identifiant unique pour chaque DEM. Tous les noms de DEM doivent être uniques, qu'ils soient sur les mêmes hôtes ou sur différents hôtes.
Nom d'utilisateur	Au format DOMAIN\username, entrez le compte de service. Le compte doit être un compte de domaine avec des privilèges d'administrateur local sur le serveur Windows laaS.
Mot de passe	Entrez le mot de passe du compte.
Description de l'instance	Si nécessaire, entrez une explication des workflows associés à chaque DEM.
Chemin d'installation	<p>Gardez cette option désactivée pour accepter la valeur par défaut %ProgramFiles(x86)%\VMware ou entrez un autre emplacement.</p> <p>Si vous installez plusieurs composants laaS sur la même machine Windows, installez-les sous le même chemin d'installation.</p>

Agents

Sur la page Agents, vous créez la liaison entre vRealize AutomationlaaS et les ressources de virtualisation sur lesquelles l'infrastructure est déployée. Vous sélectionnez un type d'agent et indiquez les détails du point de terminaison correspondant.

- Plusieurs agents du même type ou de types différents sont pris en charge.
- Vous pouvez installer les agents sur le même serveur ou sur des serveurs distincts.
- Lorsqu'ils sont sur le même serveur, jusqu'à 25 agents de tout type sont pris en charge.
- Lorsque plusieurs agents du même type se trouvent sur le même serveur, chaque agent doit avoir un nom unique et un point de terminaison différent.
- Pour la haute disponibilité, vous pouvez installer un agent du même type, du même nom et du même point de terminaison sur des serveurs distincts.
- vSphere est généralement l'un de ces types d'agents.
- Vous pouvez ajouter des agents après l'installation.

Types d'agent

Tableau 1-19. vSphere

Configuration	Description
Type d'agent	Dans le menu déroulant, sélectionnez vSphere.
Nom d'hôte laaS	Dans le menu déroulant, sélectionnez le nom de domaine complet de la machine Windows laaS qui héberge l'agent.
Nom de l'agent	Saisissez un identifiant unique, sauf si vous ajoutez un nom d'agent et un point de terminaison identiques sur des serveurs distincts pour la haute disponibilité.
Point de terminaison	Entrez un nom pour le point de terminaison vSphere.

Tableau 1-19. vSphere (suite)

Configuration	Description
Chemin d'installation	<p>Gardez cette option désactivée pour accepter la valeur par défaut %ProgramFiles(x86)%\VMware ou entrez un autre emplacement.</p> <p>Si vous installez plusieurs composants IaaS sur la même machine Windows, installez-les sous le même chemin d'installation.</p>
Nom d'utilisateur	Au format DOMAIN\username, entrez le compte de service. Le compte doit être un compte de domaine avec des privilèges d'administrateur local sur le serveur Windows IaaS.
Mot de passe	Entrez le mot de passe du compte.

Tableau 1-20. EPI PowerShell

Configuration	Description
Type d'agent	Dans le menu déroulant, sélectionnez EpiPowerShell.
Nom d'hôte IaaS	Dans le menu déroulant, sélectionnez le nom de domaine complet de la machine Windows IaaS qui héberge l'agent.
Nom de l'agent	Saisissez un identifiant unique, sauf si vous ajoutez un nom d'agent et un point de terminaison identiques sur des serveurs distincts pour la haute disponibilité.
Type	Dans le menu déroulant, sélectionnez le nom du provisionnement que le point de terminaison EPiServer héberge.
Serveur	Entrez le nom de domaine complet de l'EPiServer.
Chemin d'installation	<p>Gardez cette option désactivée pour accepter la valeur par défaut %ProgramFiles(x86)%\VMware ou entrez un autre emplacement.</p> <p>Si vous installez plusieurs composants IaaS sur la même machine Windows, installez-les sous le même chemin d'installation.</p>
Nom d'utilisateur	Au format DOMAIN\username, entrez le compte de service. Le compte doit être un compte de domaine avec des privilèges d'administrateur local sur le serveur Windows IaaS.
Mot de passe	Entrez le mot de passe du compte.

Tableau 1-21. HyperV

Configuration	Description
Type d'agent	Dans le menu déroulant, sélectionnez HyperV.
Nom d'hôte IaaS	Dans le menu déroulant, sélectionnez le nom de domaine complet de la machine Windows IaaS qui héberge l'agent.
Nom de l'agent	Saisissez un identifiant unique, sauf si vous ajoutez un nom d'agent et un point de terminaison identiques sur des serveurs distincts pour la haute disponibilité.
Nom d'utilisateur	Entrez le compte de connexion à l'instance du point de terminaison HyperV.
Mot de passe	Entrez le mot de passe du compte.

Tableau 1-21. HyperV (suite)

Configuration	Description
Chemin d'installation	<p>Gardez cette option désactivée pour accepter la valeur par défaut %ProgramFiles(x86)%\VMware ou entrez un autre emplacement.</p> <p>Si vous installez plusieurs composants IaaS sur la même machine Windows, installez-les sous le même chemin d'installation.</p>
Nom d'utilisateur	Au format DOMAIN\username, entrez le compte de service. Le compte doit être un compte de domaine avec des privilèges d'administrateur local sur le serveur Windows IaaS.
Mot de passe	Entrez le mot de passe du compte.

Tableau 1-22. VDI PowerShell

Configuration	Description
Type d'agent	Dans le menu déroulant, sélectionnez VdiPowerShell.
Nom d'hôte IaaS	Dans le menu déroulant, sélectionnez le nom de domaine complet de la machine Windows IaaS qui héberge l'agent.
Nom de l'agent	Saisissez un identifiant unique, sauf si vous ajoutez un nom d'agent et un point de terminaison identiques sur des serveurs distincts pour la haute disponibilité.
Type	Le type de point de terminaison est défini par défaut sur XenDesktop et ne peut pas être modifié.
Serveur	Entrez le nom de domaine complet du point de terminaison XenDesktop.
Version de XenDesktop	Dans le menu déroulant, sélectionnez la version.
Chemin d'installation	<p>Gardez cette option désactivée pour accepter la valeur par défaut %ProgramFiles(x86)%\VMware ou entrez un autre emplacement.</p> <p>Si vous installez plusieurs composants IaaS sur la même machine Windows, installez-les sous le même chemin d'installation.</p>
Nom d'utilisateur	Au format DOMAIN\username, entrez le compte de service. Le compte doit être un compte de domaine avec des privilèges d'administrateur local sur le serveur Windows IaaS.
Mot de passe	Entrez le mot de passe du compte.

Tableau 1-23. Xen

Configuration	Description
Type d'agent	Dans le menu déroulant, sélectionnez Xen.
Nom d'hôte IaaS	Dans le menu déroulant, sélectionnez le nom de domaine complet de la machine Windows IaaS qui héberge l'agent.
Nom de l'agent	Saisissez un identifiant unique, sauf si vous ajoutez un nom d'agent et un point de terminaison identiques sur des serveurs distincts pour la haute disponibilité.
Nom d'utilisateur	Entrez le compte de connexion à l'instance du point de terminaison Xen.
Mot de passe	Entrez le mot de passe du compte.

Tableau 1-23. Xen (suite)

Configuration	Description
Chemin d'installation	<p>Gardez cette option désactivée pour accepter la valeur par défaut %ProgramFiles(x86)%\VMware ou entrez un autre emplacement.</p> <p>Si vous installez plusieurs composants laaS sur la même machine Windows, installez-les sous le même chemin d'installation.</p>
Nom d'utilisateur	Au format DOMAIN\username, entrez le compte de service. Le compte doit être un compte de domaine avec des privilèges d'administrateur local sur le serveur Windows laaS.
Mot de passe	Entrez le mot de passe du compte.

Tableau 1-24. WMI

Configuration	Description
Type d'agent	Dans le menu déroulant, sélectionnez WMI.
Nom d'hôte laaS	Dans le menu déroulant, sélectionnez le nom de domaine complet de la machine Windows laaS qui héberge l'agent.
Nom de l'agent	Saisissez un identifiant unique, sauf si vous ajoutez un nom d'agent et un point de terminaison identiques sur des serveurs distincts pour la haute disponibilité.
Chemin d'installation	<p>Gardez cette option désactivée pour accepter la valeur par défaut %ProgramFiles(x86)%\VMware ou entrez un autre emplacement.</p> <p>Si vous installez plusieurs composants laaS sur la même machine Windows, installez-les sous le même chemin d'installation.</p>
Nom d'utilisateur	Au format DOMAIN\username, entrez le compte de service. Le compte doit être un compte de domaine avec des privilèges d'administrateur local sur le serveur Windows laaS.
Mot de passe	Entrez le mot de passe du compte.

Tableau 1-25. Tester

Configuration	Description
Type d'agent	Dans le menu déroulant, sélectionnez Tester.
Nom d'hôte laaS	Dans le menu déroulant, sélectionnez le nom de domaine complet de la machine Windows laaS qui héberge l'agent.
Nom de l'agent	Saisissez un identifiant unique, sauf si vous ajoutez un nom d'agent et un point de terminaison identiques sur des serveurs distincts pour la haute disponibilité.
Chemin d'installation	<p>Gardez cette option désactivée pour accepter la valeur par défaut %ProgramFiles(x86)%\VMware ou entrez un autre emplacement.</p> <p>Si vous installez plusieurs composants laaS sur la même machine Windows, installez-les sous le même chemin d'installation.</p>

Tableau 1-25. Tester (suite)

Configuration	Description
Nom d'utilisateur	Au format DOMAIN\username, entrez le compte de service. Le compte doit être un compte de domaine avec des privilèges d'administrateur local sur le serveur Windows IaaS.
Mot de passe	Entrez le mot de passe du compte.

Certificat vRealize Appliance

Sur la page Certificat vRealize Appliance, vous créez ou sélectionnez le certificat d'authentification utilisé par le dispositif vRealize Automation. Lorsque le certificat est autosigné, les utilisateurs finaux peuvent le voir et le confirmer lorsqu'ils se connectent à vRealize Automation dans un navigateur.

Configuration	Description
Action de certificat	<p>Conserver l'existant</p> <p>Utilisez le certificat qui existe déjà sur ce dispositif vRealize Automation. Vérifiez les détails des entrées ci-dessous, telles que le numéro de série et l'empreinte digitale.</p> <p>Générer un certificat</p> <p>Utilisez l'Assistant pour générer un certificat autosigné du dispositif vRealize Automation.</p> <p>Générer une demande de signature</p> <p>Créez un fichier de demande de signature de certificat (CSR) pour votre autorité de certification (CA). Une CSR permet à votre autorité de certification de créer un certificat avec les valeurs correctes que vous pouvez importer.</p> <ol style="list-style-type: none"> 1 Entrez une organisation, une unité d'organisation et un code pays (voir ci-dessous). 2 Cliquez sur Générer une demande de signature. 3 Pour télécharger le fichier CSR pour votre autorité de certification, cliquez sur le lien qui s'affiche. <p>Importer</p> <p>Identifiez un fichier de certificat au format PEM, ajoutez-le au magasin approprié à l'aide de l'assistant et chargez-le pour une utilisation avec vRealize Automation.</p> <p>À moins d'importer un certificat créé à partir de votre CSR, cette option vous oblige à entrer la clé privée du certificat, la phrase secrète de la clé privée (le cas échéant) et la chaîne de certificats.</p> <p>Lorsque vous importez un PEM fourni par une autorité de certification et qui a été créé à partir de votre CSR, ne remplissez pas les champs de la clé privée et de la phrase secrète.</p>
Nom commun	<p>Nom de domaine complet du dispositif vRealize Automation.</p> <p>Dans les déploiements d'entreprise à haute disponibilité avec un équilibrage de charge devant plusieurs dispositifs, cette entrée est le nom de domaine complet de l'équilibrage de charge.</p>

Configuration	Description
Organisation	Entrez un texte pour définir le plus grand département ou la plus grande unité commerciale.
Unité d'organisation	Entrez un texte pour définir le plus petit département ou la plus petite unité commerciale.
Code pays	Entrez une abréviation pour votre pays d'activité.
Série	Identifiant alphanumérique unique
Empreinte digitale	Chaîne alphanumérique unique utilisée pour identifier un certificat ou pour comparer les certificats entre eux
Date de début de validité	Horodatage à partir duquel le certificat peut être utilisé
Date de fin de validité	Horodatage à partir duquel le certificat ne peut plus être utilisé

Certificat Web

Sur la page Certificat Web, vous créez ou sélectionnez le certificat d'authentification utilisé par le serveur Web IaaS. Le dispositif vRealize Automation se connecte au serveur Web et doit s'y authentifier et l'approuver.

Configuration	Description
Action de certificat	Conserver l'existant
	Utilisez le certificat qui existe déjà sur ce serveur Web IaaS. Vérifiez les détails des entrées ci-dessous, telles que le numéro de série et l'empreinte digitale.
	Générer un certificat
	Utilisez l'assistant pour générer un certificat autosigné du serveur Web IaaS.
	Générer une demande de signature
	<p>Créez un fichier de demande de signature de certificat (CSR) pour votre autorité de certification (CA). Une CSR permet à votre autorité de certification de créer un certificat avec les valeurs correctes que vous pouvez importer.</p> <ol style="list-style-type: none"> 1 Entrez une organisation, une unité d'organisation et un code pays (voir ci-dessous). 2 Cliquez sur Générer une demande de signature. 3 Pour télécharger le fichier CSR pour votre autorité de certification, cliquez sur le lien qui s'affiche.
	Importer
	<p>Identifiez un fichier de certificat au format PEM, ajoutez-le au magasin approprié à l'aide de l'assistant et chargez-le pour une utilisation avec vRealize Automation.</p> <p>À moins d'importer un certificat créé à partir de votre CSR, cette option vous oblige à entrer la clé privée du certificat, la phrase secrète de la clé privée (le cas échéant) et la chaîne de certificats.</p> <p>Lorsque vous importez un PEM fourni par une autorité de certification et qui a été créé à partir de votre CSR, ne remplissez pas les champs de la clé privée et de la phrase secrète.</p>

Configuration		Description
	Fournir l'empreinte numérique du certificat	Chargez un certificat que vous avez déjà ajouté au magasin approprié.
Nom commun		Le nom de domaine complet du serveur Web IaaS. Dans les déploiements d'entreprise à haute disponibilité avec un équilibrage de charge devant plusieurs serveurs Web, cette entrée est le nom de domaine complet de l'équilibrage de charge.
Organisation		Entrez un texte pour définir le plus grand département ou la plus grande unité commerciale.
Unité d'organisation		Entrez un texte pour définir le plus petit département ou la plus petite unité commerciale.
Code pays		Entrez une abréviation pour votre pays d'activité.
Série		Identifiant alphanumérique unique
Empreinte digitale		Chaîne alphanumérique unique utilisée pour identifier un certificat ou pour comparer les certificats entre eux
Date de début de validité		Horodatage à partir duquel le certificat peut être utilisé
Date de fin de validité		Horodatage à partir duquel le certificat ne peut plus être utilisé

Certificat du service de gestionnaire

(Déploiements d'entreprise uniquement) Sur la page Certificat du service de gestionnaire, vous créez ou sélectionnez le certificat d'authentification utilisé par l'hôte du service de gestionnaire vRealize Automation IaaS. Les autres serveurs Windows IaaS se connectent à l'hôte du service de gestionnaire et doivent s'y authentifier et l'approuver.

Cette page apparaît uniquement lorsque vous hébergez le service de gestionnaire sur une machine distincte du serveur Web IaaS. Lorsqu'ils sont hébergés sur la même machine, le certificat Web fournit une authentification pour les deux rôles.

Configuration		Description
Action de certificat	Conserver l'existant	Utilisez le certificat qui existe déjà sur cet hôte du service de gestionnaire IaaS. Vérifiez les détails des entrées ci-dessous, telles que le numéro de série et l'empreinte digitale.
	Générer un certificat	Utilisez l'assistant pour générer un certificat autosigné de l'hôte du service de gestionnaire IaaS.

Configuration	Description
Générer une demande de signature	<p>Créez un fichier de demande de signature de certificat (CSR) pour votre autorité de certification (CA). Une CSR permet à votre autorité de certification de créer un certificat avec les valeurs correctes que vous pouvez importer.</p> <ol style="list-style-type: none"> 1 Entrez une organisation, une unité d'organisation et un code pays (voir ci-dessous). 2 Cliquez sur Générer une demande de signature. 3 Pour télécharger le fichier CSR pour votre autorité de certification, cliquez sur le lien qui s'affiche.
Importer	<p>Identifiez un fichier de certificat au format PEM, ajoutez-le au magasin approprié à l'aide de l'assistant et chargez-le pour une utilisation avec vRealize Automation.</p> <p>À moins d'importer un certificat créé à partir de votre CSR, cette option vous oblige à entrer la clé privée du certificat, la phrase secrète de la clé privée (le cas échéant) et la chaîne de certificats.</p> <p>Lorsque vous importez un PEM fourni par une autorité de certification et qui a été créé à partir de votre CSR, ne remplissez pas les champs de la clé privée et de la phrase secrète.</p>
Fournir l'empreinte numérique du certificat	Chargez un certificat que vous avez déjà ajouté au magasin approprié.
Nom commun	<p>Le nom de domaine complet de l'hôte du service de gestionnaire IaaS.</p> <p>Dans les déploiements d'entreprise à haute disponibilité avec un équilibrage de charge devant plusieurs hôtes du service de gestionnaire, cette entrée est le nom de domaine complet de l'équilibrage de charge.</p>
Organisation	Entrez un texte pour définir le plus grand département ou la plus grande unité commerciale.
Unité d'organisation	Entrez un texte pour définir le plus petit département ou la plus petite unité commerciale.
Code pays	Entrez une abréviation pour votre pays d'activité.
Série	Identifiant alphanumérique unique
Empreinte digitale	Chaîne alphanumérique unique utilisée pour identifier un certificat ou pour comparer les certificats entre eux
Date de début de validité	Horodatage à partir duquel le certificat peut être utilisé
Date de fin de validité	Horodatage à partir duquel le certificat ne peut plus être utilisé

Équilibrages de charge

(Déploiements d'entreprise uniquement) Sur la page Équilibrages de charge, prenez le temps de configurer les équilibrages de charge du pool correct des systèmes membres de vRealize Automation.

La liste des équilibrages de charge est fournie à titre informatif seulement. En fonction de vos entrées précédentes dans l'assistant, cette liste répertorie chaque équilibrage de charge de votre déploiement, ainsi que les membres, leur rôle de composant, le nom de domaine complet et le numéro de port.

Prenez le temps d'utiliser la liste pendant que vous vous connectez à vos équilibrages de charge pour ajouter des membres vRealize Automation et ouvrir des ports.

Pour plus d'informations sur la façon d'équilibrer la charge d'hôtes, reportez-vous à [Équilibrage de charge de vRealize Automation](#).

Validation

Sur la page Validation, vérifiez que l'installation de vRealize Automation peut continuer.

Pour vérifier que tous les composants, rôles et comptes vRealize Automation sont corrects et que les systèmes peuvent s'authentifier mutuellement, cliquez sur **Valider**. Le processus peut prendre une demi-heure ou plus en fonction de votre environnement.

Si des erreurs se produisent, développez l'élément de la ligne ayant échoué et apportez les corrections en fonction de l'état et des messages affichés. Vous ne pouvez pas poursuivre l'installation de vRealize Automation tant que la validation n'a pas réussi.

Créer des snapshots

Sur la page Créer des snapshots, vous pouvez prendre des snapshots de machine virtuelle de tous les composants vRealize Automation avant de poursuivre l'installation.

Même si la validation a réussi, nous vous encourageons vivement à envisager des problèmes inattendus autour de l'installation. Avant de commencer l'installation, utilisez votre client vSphere pour prendre un snapshot de chaque dispositif vRealize Automation et serveur Windows IaaS. Dans le cas contraire, vous devrez entrer à nouveau tous les paramètres de l'assistant pour revenir à ce stade.

Si vous disposez de suffisamment de ressources, vous pouvez prendre des snapshots de machines virtuelles en cours d'exécution. Il est cependant recommandé de les arrêter au préalable.

- 1 Dans le coin supérieur droit de l'assistant d'installation, cliquez sur **Déconnexion**.

Important Si vous fermez l'assistant en utilisant une autre commande que **Déconnexion**, vous ne pourrez plus rouvrir l'assistant.

- 2 Dans vSphere, fermez le système d'exploitation invité de chaque dispositif vRealize Automation et serveur Windows IaaS.
- 3 Cliquez avec le bouton droit sur les machines virtuelles et sélectionnez **Prendre un snapshot**.

- 4 Nom du snapshot.
- 5 Pour inclure la mémoire de machine dans le snapshot, sélectionnez **Snapshot de mémoire de la machine virtuelle**.
- 6 Cliquez sur **OK**.
Attendez que les snapshots soient créés.
- 7 Mettez sous tension le système d'exploitation invité de chaque dispositif vRealize Automation et serveur Windows IaaS.
- 8 Revenez à la page Snapshot de l'assistant d'installation en vous connectant à nouveau en tant qu'utilisateur racine.
`https://vrealize-automation-appliance-FQDN:5480`

Détails de l'installation

Sur la page Détails de l'installation, vous démarrez l'installation de vRealize Automation ou effectuez une nouvelle tentative si des problèmes sont survenus.

Info-bulle Une erreur d'installation occasionnelle concernant les clés de la base de données en double a été signalée. Si vous souhaitez éviter cette erreur, exécutez l'instruction de mise à jour SQL suivante sur la base de données vPostgres intégrée avant de cliquer sur **Installer**.

```
update cluster_commands set output='' where type like '%install%';
```

Pour commencer l'installation, cliquez sur **Installer**. Selon votre environnement, l'installation peut prendre une heure ou plus.

Pendant ou après l'installation, vous pouvez cliquer sur le bouton **Collecter les journaux**.

- Lorsque vous collectez les journaux, un lien de téléchargement de fichier ZIP s'affiche au-dessus du tableau d'état.
- Lorsque vous collectez les journaux plusieurs fois, chaque collecte remplace la précédente.

Si vous souhaitez les tout derniers journaux, téléchargez-les avant de cliquer sur **Collecter les journaux**.

Si des problèmes surviennent, l'assistant arrête l'installation et affiche des messages pour vous aider à corriger les erreurs. Après avoir évalué les messages et pris note des corrections à effectuer, vous pourrez ou non avoir besoin des snapshots que vous avez créés.

Ne pas restaurer les snapshots

Si l'assistant active l'option **Échec de la tentative**, vous pouvez effectuer des corrections, puis relancer l'installation sans restaurer aucune machine avec des snapshots.

Après avoir effectué des corrections, cliquez sur **Échec de la tentative**.

Restaurer les serveurs Windows IaaS aux snapshots

Si l'assistant active l'option **Réessayer tous les IaaS**, procédez comme suit.

- 1 Dans vSphere, restaurez toutes les machines Windows IaaS avec les snapshots pris sur la page précédente de l'assistant.
- 2 Si les snapshots ont été pris après un arrêt, mettez sous tension les systèmes d'exploitation invités.
- 3 Si vous avez utilisé un serveur SQL externe, supprimez la base de données SQL vRealize Automation.
- 4 Effectuez des corrections.
- 5 Cliquez sur **Réessayer tous les IaaS**.

Si **Réessayer tous les IaaS** échoue avec une erreur indiquant qu'un élément avec la même clé a déjà été ajouté, exécutez l'instruction de mise à jour SQL suivante sur la base de données vPostgres intégrée. Ensuite, cliquez de nouveau sur **Réessayer tous les IaaS**.

```
update cluster_commands set output='' where type like '%install%';
```

Restaurer les dispositifs et les serveurs Windows IaaS aux snapshots

Si l'assistant affiche des messages à propos du dispositif vRealize Automation, procédez comme suit.

- 1 Dans vSphere, restaurez tous les dispositifs vRealize Automation et toutes les machines Windows IaaS avec les snapshots pris sur la page précédente de l'assistant.
- 2 Si les snapshots ont été pris après un arrêt, mettez sous tension les systèmes d'exploitation invités.
- 3 Si vous avez utilisé un serveur SQL externe, supprimez la base de données SQL vRealize Automation.
- 4 Effectuez des corrections.
- 5 Revenez à la page Assistant d'installation en vous connectant à nouveau en tant qu'utilisateur racine.

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

- 6 Revenez à la page Détails de l'installation, puis cliquez sur **Installer**.

Attribution de licence

Sur la page Attribution de licence, vous entrez une clé pour activer le produit vRealize Automation installé.

Dans le champ **Nouvelle clé de licence**, saisissez votre clé et cliquez sur **Envoyer la clé**. Vous pouvez soumettre plusieurs clés séparément, y compris des clés pour des installations autonomes de vRealize Automation, vRealize Suite, vRealize Business for Cloud et vRealize Code Stream.

Télémétrie

Sur la page Télémétrie, vous décidez si vRealize Automation peut envoyer ou non des statistiques d'utilisation à VMware dans le cadre du Programme d'amélioration du produit.

Activez ou désactivez l'option pour rejoindre le Programme d'amélioration du produit (CEIP).

Pour plus d'informations, consultez le [Programme d'amélioration du produit](#).

Options après installation

Sur la page Options après installation, vous disposez d'options de création de données vRealize Automation ou de migration des anciennes données de déploiement vers votre nouvelle installation.

- L'option **Configurer le contenu initial** crée un utilisateur local du locataire par défaut. Cet utilisateur local peut démarrer le processus de configuration du locataire par défaut.

Pour activer cette option, vous devez avoir ajouté au moins un point de terminaison vSphere au préalable, sur la page Agents de l'assistant d'installation.
- L'option **Migrer un déploiement** transfère vos anciennes données vRealize Automation vers le déploiement venant d'être installé. La migration conserve les éléments essentiels tels que les groupes, les Blueprints et les points de terminaison.
- L'option **Continuer** vous renvoie à la fin de l'Assistant d'installation.

Configuration du contenu initial

Sur la page Configuration du contenu initial, vous créez un nouvel utilisateur locataire par défaut vRealize Automation local qui peut commencer un workflow de contenu pour un point de terminaison vSphere.

Note Cette option est uniquement disponible si vous avez ajouté au moins un point de terminaison vSphere au préalable, sur la page Agents.

Le nouveau nom d'utilisateur local est configurationadmin. vRealize Automation accorde les privilèges suivants à configurationadmin.

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

Entrez et confirmez un mot de passe de connexion pour configurationadmin. Pour générer un élément de catalogue afin que configurationadmin puisse démarrer le processus de configuration après la connexion au locataire par défaut, cliquez sur **Créer du contenu initial**.

Configuration de la migration

Sur la page Configuration de la migration, vous pouvez démarrer le transfert d'un ancien déploiement vRealize Automation vers le déploiement que vous venez d'installer.

Avant d'effectuer la migration d'un ancien déploiement, appliquez les directives suivantes.

- Vérifiez soigneusement le guide de migration vRealize Automation associé à la version de votre ancien déploiement. Les conditions préalables et d'autres détails peuvent varier.
- Migrez les anciens locataires et magasins d'identités vers VMware Identity Manager sur le nouveau déploiement.
- Clonez l'ancienne base de données SQL Server IaaS et restaurez-la sur la base de données IaaS du nouveau déploiement. Notez le nom de la base de données clonée.
- Obtenez et notez la clé de chiffrement de l'ancienne base de données SQL Server IaaS.
- Créez et notez une nouvelle phrase secrète afin de chiffrer à nouveau les données migrées.
- Notez le nom de domaine complet et les informations d'identification racine de l'ancien équilibrage de charge ou dispositif vRealize Automation.
- Notez les informations d'identification racine du nouveau déploiement.

Les interfaces d'installation standard de vRealize Automation

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

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

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

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

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

Utilisation des interfaces standard pour des déploiements minimaux

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

Liste de contrôle pour un déploiement minimal

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

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

Tableau 1-26. Liste de contrôle pour un déploiement minimal

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

Configurer le dispositif vRealize Automation

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

Conditions préalables

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

Procédure

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

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

Continuez après l'affichage éventuel des avertissements de certificat.

- 2 Si l'assistant d'installation s'affiche, annulez-le afin de pouvoir accéder à l'interface de gestion plutôt qu'à l'assistant.

- 3 Sélectionnez **Admin > Paramètres de l'heure** et définissez la source de synchronisation de l'heure.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- 11** Saisissez les informations sur votre licence.

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

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

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

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

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

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

Résultats

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

Étape suivante

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

Installation des composants IaaS

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

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

Activer la synchronisation de l'heure sur le serveur Windows

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

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

Procédure

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

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

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

```
VMwareToolboxCmd.exe timesync status
```

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

```
VMwareToolboxCmd.exe timesync enable
```

Certificats IaaS

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

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

Installer les composants d'infrastructure

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

Conditions préalables

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

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

Procédure

1 Télécharger le programme d'installation de vRealize AutomationIaaS

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

2 Sélectionner le type d'installation

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

3 Vérifier les conditions préalables

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

4 Spécifier les paramètres de serveur et de compte

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

5 Spécifier les gestionnaires et les agents

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

6 Enregistrer les composants IaaS

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

7 Terminer l'installation

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

Télécharger le programme d'installation de vRealize AutomationIaaS

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

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

Conditions préalables

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

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

Procédure

- 1 Connectez-vous au serveur IaaS Windows en utilisant un compte ayant des droits d'administrateur.
- 2 Ouvrez un navigateur Web directement à l'URL du programme d'installation du dispositif vRealize Automation.
`https://vrealize-automation-appliance-FQDN:5480/installer`
- 3 Cliquez sur **Programme d'installation d'IaaS**.
- 4 Enregistrez `setup__vrealize-automation-appliance-FQDN@5480` sur le serveur Windows.
Ne modifiez pas le nom de fichier du programme d'installation. Il est utilisé pour connecter l'installation au dispositif vRealize Automation

Sélectionner le type d'installation

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

Conditions préalables

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

Procédure

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

6 Cliquez sur **Suivant**.

7 Sélectionnez **Installation complète** sur la page **Type d'installation** si vous créez un déploiement minimal et cliquez sur **Suivant**.

Vérifier les conditions préalables

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

Conditions préalables

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

Procédure

1 Terminez la vérification des conditions préalables.

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

2 Cliquez sur **Suivant**.

Résultats

La machine répond aux conditions préalables pour l'installation.

Spécifier les paramètres de serveur et de compte

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

Conditions préalables

[Vérifier les conditions préalables.](#)

Procédure

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

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

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

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

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

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

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

4 Acceptez la valeur par défaut dans la zone de texte **Nom de la base de données** ou entrez le nom correspondant, au besoin.**5** Sélectionnez la méthode d'authentification.

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

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

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

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

7 Cliquez sur **Suivant**.

Spécifier les gestionnaires et les agents

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

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

Conditions préalables

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

Procédure

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

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

Enregistrer les composants IaaS

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

Conditions préalables

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

Procédure

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

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

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

9 Cliquez sur **Suivant**.

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

Terminer l'installation

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

Conditions préalables

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

Procédure

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

Résultats

L'installation est maintenant terminée.

Étape suivante

[Vérifier les services laaS.](#)

Utilisation des interfaces standard pour les déploiements distribués

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

Liste de contrôle d'un déploiement distribué

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

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

Tableau 1-27. 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.	Préparation à l'installation de vRealize Automation
<input type="checkbox"/> Planifiez et obtenez vos certificats SSL.	Exigences de confiance du certificat dans un déploiement distribué
<input type="checkbox"/> Déployez le serveur du dispositif vRealize Automation principal, et tous les dispositifs supplémentaires nécessaires pour la redondance et la haute disponibilité.	Déployer le dispositif vRealize Automation
<input type="checkbox"/> Configurez votre équilibrage de charge pour gérer le trafic des dispositifs vRealize Automation.	Configuration de votre équilibrage de charge
<input type="checkbox"/> Configurez le serveur du dispositif vRealize Automation principal, et tous les dispositifs supplémentaires que vous avez déployés pour la redondance et la haute disponibilité.	Configuration de dispositifs pour vRealize Automation
<input type="checkbox"/> Configurez votre équilibrage de charge pour gérer le trafic des composants IaaS vRealize Automation et installez les composants IaaS vRealize Automation.	Installer les composants IaaS dans une configuration distribuée
<input type="checkbox"/> Le cas échéant, installez les agents pour l'intégration à des systèmes externes.	Installation d'agents vRealize Automation
<input type="checkbox"/> Configurez le locataire par défaut et fournissez la licence IaaS.	Configurer l'accès au locataire par défaut

vRealize Orchestrator

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

Pour obtenir des informations sur la connexion de vRealize Automation et de vRealize Orchestrator, reportez-vous à [Plug-in VMware 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.

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 éligibles pour tout nouveau trafic.

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

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

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

Exigences de confiance du certificat dans un déploiement distribué

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

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

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

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

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

Certificats générés par le système

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

Si vous devez mettre à jour des certificats autosignés générés par le système avec des certificats fournis par l'utilisateur ou l'autorité de certification, reportez-vous à la section [Mise à jour des certificats vRealize Automation](#).

Fournir vos propres certificats

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

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

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

Équilibrages de charge

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

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

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

Conditions d'approbation des certificats

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

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

Approbation de certificat et programme d'installation standard

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

- Hôtes IaaS Web et Manager Service

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

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

- Hôtes IaaS DEM Orchestrator, DEM Worker et agent proxy

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

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

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

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

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

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

Conditions préalables

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

Procédure

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

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

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

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

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

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

- a Sélectionnez **Ajouter/Supprimer un composant logiciel enfichable**.
- b Sélectionnez **Certificats**.

- c Sélectionnez **Ordinateur local**.
- d Ouvrez les fichiers de certificats que vous avez précédemment importés et copiez les empreintes numériques.

Étape suivante

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

Feuilles d'activité d'installation

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

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

Tableau 1-28. Dispositif vRealize Automation

Variable	Ma valeur	Exemple
Nom de domaine complet du dispositif vRealize Automation principal		automation.mycompany.com
Adresse IP du dispositif principal vRealize Automation Pour référence uniquement ; n'entrez pas d'adresses IP		123.234.1.105
Nom de domaine complet du dispositif vRealize Automation supplémentaire		automation2.mycompany.com
Adresse IP du dispositif vRealize Automation supplémentaire Pour référence uniquement ; n'entrez pas d'adresses IP		123.234.1.106
Nom de domaine complet de l'équilibrage de charge du dispositif vRealize Automation		automation-balance.mycompany.com
Adresse IP de l'équilibrage de charge du dispositif vRealize Automation Pour référence uniquement ; n'entrez pas d'adresses IP		123.234.1.201
Nom d'utilisateur de l'interface de gestion (https://appliance-FQDN:5480)	racine (par défaut)	root
Mot de passe de l'interface de gestion		admin123

Tableau 1-28. Dispositif vRealize Automation (suite)

Variable	Ma valeur	Exemple
Locataire par défaut	vsphere.local (par défaut)	vsphere.local
Nom d'utilisateur du locataire par défaut	administrator@vsphere.local (par défaut)	administrator@vsphere.local
Mot de passe par défaut du locataire		login123

Tableau 1-29. Serveurs Windows IaaS

Variable	Ma valeur	Exemple
Serveur Web IaaS principal avec nom de domaine complet de Model Manager Data		web.mycompany.com
Serveur Web IaaS principal avec adresse IP de Model Manager Data Pour référence uniquement ; n'entrez pas d'adresses IP		123.234.1.107
Nom de domaine complet du serveur Web IaaS supplémentaire		web2.mycompany.com
Adresse IP du serveur Web IaaS supplémentaire Pour référence uniquement ; n'entrez pas d'adresses IP		123.234.1.108
Nom de domaine complet de l'équilibrage de charge du serveur Web IaaS		web-balance.mycompany.com
Adresse IP de l'équilibrage de charge du serveur Web IaaS Pour référence uniquement ; n'entrez pas d'adresses IP		123.234.1.202
Nom de domaine complet de l'hôte IaaS Manager Service actif		mgr-svc.mycompany.com
Adresses IP de l'hôte IaaS Manager Service actif Pour référence uniquement ; n'entrez pas d'adresses IP		123.234.1.109
Nom de domaine complet de l'hôte IaaS Manager Service passif		mgr-svc2.mycompany.com
Adresses IP de l'hôte IaaS Manager Service passif Pour référence uniquement ; n'entrez pas d'adresses IP		123.234.1.110
Nom de domaine complet de l'équilibrage de charge de l'hôte IaaS Manager Service		mgr-svc-balance.mycompany.com

Tableau 1-29. Serveurs Windows IaaS (suite)

Variable	Ma valeur	Exemple
Adresses IP de l'équilibrage de charge de l'hôte IaaS Manager Service Pour référence uniquement ; n'entrez pas d'adresses IP		123.234.203
Pour les services IaaS, compte de domaine avec droits d'administrateur sur les hôtes		SUPPORT\provisioner
Mot de passe du compte		login123

Tableau 1-30. Base de données IaaS SQL Server

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

Tableau 1-31. Instances d'IaaS Distributed Execution Manager

Variable	Ma valeur	Exemple
Nom de domaine complet de l'hôte DEM		dem.mycompany.com
Adresses IP de l'hôte DEM Pour référence uniquement ; n'entrez pas d'adresses IP		123.234.1.111
Nom de domaine complet de l'hôte DEM		dem2.mycompany.com
Adresses IP de l'hôte DEM Pour référence uniquement ; n'entrez pas d'adresses IP		123.234.1.112
Nom unique du composant DEM Orchestrator		Orchestrator-1
Nom unique du composant DEM Orchestrator		Orchestrator-2
Nom unique du composant DEM Worker		Worker-1
Nom unique du composant DEM Worker		Worker-2

Tableau 1-31. Instances d'IaaS Distributed Execution Manager (suite)

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

Configuration de votre équilibrage de charge

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

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

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

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

Pour en savoir plus sur l'équilibrage de charge, reportez-vous à [Équilibrage de charge dans vRealize Automation](#).

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

Configuration de dispositifs pour vRealize Automation

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

Configurez le premier dispositif vRealize Automation dans un cluster

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

Conditions préalables

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

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

Procédure

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

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

Continuez après l'affichage éventuel des avertissements de certificat.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8 Configurez les paramètres SSO.

9 Cliquez sur **Services**.

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

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

10 Saisissez les informations sur votre licence.

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

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

11 Cliquez sur **Messagerie**. Les paramètres de configuration et l'état de la messagerie pour votre dispositif s'affichent. Ne modifiez pas ces paramètres.

12 Cliquez sur l'onglet **Télémétrie** pour indiquer si vous souhaitez participer au programme d'amélioration du produit de VMware (CEIP).

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

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

13 Cliquez sur **Enregistrer les paramètres**.

14 Vérifiez que vous pouvez vous connecter à vRealize Automation.

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

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

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

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

Configuration d'instances supplémentaires du dispositif vRealize Automation

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

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

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

Ajouter un autre dispositif vRealize Automation au cluster

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

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

Active Directory—Chaque instance du dispositif vRealize Automation inclut un connecteur qui prend en charge l'authentification de l'utilisateur, bien qu'un seul connecteur soit habituellement configuré pour exécuter la synchronisation d'annuaire. Après avoir ajouté un autre dispositif, n'oubliez pas de configurer un second connecteur qui correspond au dispositif ajouté. Le second connecteur se connecte à votre fournisseur d'identité et pointe vers le même dispositif Active Directory. De cette manière, si le premier dispositif échoue, le second prend en charge la gestion de l'authentification de l'utilisateur.

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

Conditions préalables

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

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

- Créez le nouveau nœud de dispositif. Reportez-vous à [Déployer le dispositif vRealize Automation](#).
- Vérifiez que l'équilibrage de charge est configuré pour une utilisation avec le nouveau dispositif.
- Vérifiez que le trafic peut franchir l'équilibrage de charge pour atteindre tous les nœuds actuels ainsi que le nouveau nœud que vous allez ajouter.

- Vérifiez que tous les services vRealize Automation sont démarrés sur les nœuds en cours.

Procédure

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

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

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

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

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

Résultats

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

Désactiver les services inutilisés

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

Conditions préalables

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

Procédure

- 1 Connectez-vous à la console du dispositif vRealize Automation.

2 Arrêtez le service vRealize Orchestrator.

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

Valider le déploiement distribué

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

Procédure

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

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

Installer les composants IaaS dans une configuration distribuée

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

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

Conditions préalables

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

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

Procédure

1 Installer des certificats IaaS

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

2 Télécharger le programme d'installation de vRealize Automation IaaS

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

3 Choisir un scénario de base de données IaaS

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

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

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

5 Installer des composants de serveur Web IaaS supplémentaires

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

6 Installer le service Active Manager Service

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

7 Installer un composant de sauvegarde Manager Service

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

8 Installation des composants Distributed Execution Manager

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

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

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

10 Vérifier les services IaaS

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

Étape suivante

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

Installer des certificats IaaS

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

Conditions préalables

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

Procédure

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

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

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

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

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

Étape suivante

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

Télécharger le programme d'installation de vRealize AutomationIaaS

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.

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

Conditions préalables

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

Procédure

- 1 (Facultatif) Activez HTTP si vous procédez à l'installation sur une machine Windows 2012.
 - a Sélectionnez **Fonctionnalités > Ajouter des fonctionnalités** depuis Server Manager.
 - b Développez **Services WCF** sous Fonctionnalités .NET Framework.
 - c Sélectionnez **Activation HTTP**.
- 2 Connectez-vous au serveur IaaS Windows en utilisant un compte ayant des droits d'administrateur.
- 3 Ouvrez un navigateur Web directement à l'URL du programme d'installation du dispositif vRealize Automation. N'utilisez pas d'adresse d'équilibrage de charge.
`https://vrealize-automation-appliance-FQDN:5480/installer`
- 4 Cliquez sur **Programme d'installation d'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

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

Étape suivante

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

Choisir un scénario de base de données IaaS

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

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

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

Tableau 1-32. Choisir un scénario de base de données IaaS

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

Créer la base de données IaaS manuellement

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

Conditions préalables

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

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

Procédure

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

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

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

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

Tableau 1-33. Valeurs de la base de données

Variable	Valeur
<i>db_server</i>	Spécifie l'instance SQL Server dans le format dbhostname[,port number]\SQL instance. 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 localhost.
<i>db_name</i>	Nom de la base de données. La valeur par défaut est vra. 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.

Tableau 1-33. Valeurs de la base de données (suite)

Variable	Valeur
<i>log_dir</i>	Chemin vers le répertoire de journaux de la base de données, en excluant la barre oblique finale.
<i>service_user</i>	Nom d'utilisateur utilisé pour exécuter Manager Service.
<i>Web_user</i>	Nom d'utilisateur utilisé pour exécuter les services Web.
<i>version_string</i>	Version de vRealize Automation, trouvée en se connectant au dispositif vRealize Automation et en cliquant dans l'onglet Mettre à jour. Par exemple, la chaîne de la version 6.1 de vRealize Automation est 6.1.0.1200.

Résultats

La base de données a été créée.

Étape suivante

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

Préparer une base de données vide

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

Conditions préalables

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

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

Procédure

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

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

Tableau 1-34. 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 `SetDatabaseSettings.sql` et modifiez-les au besoin.

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

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

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

Étape suivante

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

Créer la base de données IaaS à l'aide de l'assistant d'installation
vRealize Automation utilise une base de données Microsoft SQL Server pour mettre à jour les informations sur les machines qu'il gère et ses propres éléments et stratégies.

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

Conditions préalables

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

Procédure

- 1 Cliquez avec le bouton droit sur le fichier d'installation `setup__vrealize-automation-appliance-FQDN@5480.exe` et sélectionnez **Exécuter en tant qu'administrateur**.
- 2 Cliquez sur **Suivant**.
- 3 Acceptez le contrat de licence, puis cliquez sur **Suivant**.
- 4 Sur la page de connexion, fournissez les informations d'identification d'administrateur pour le dispositif vRealize Automation et vérifiez le certificat SSL.
 - a Entrez le nom d'utilisateur **root** et le mot de passe.
 Le mot de passe est celui que vous avez spécifié lors du déploiement du dispositif vRealize Automation.
 - b Sélectionnez **Accepter le certificat**.
 - c Cliquez sur **Afficher le certificat**.
 Comparez l'empreinte de certificat à l'empreinte définie pour le dispositif vRealize Automation. Vous pouvez afficher le certificat du dispositif vRealize Automation dans le navigateur du client si vous avez accédé à l'interface de gestion du dispositif vRealize Automation sur le port 5480.
- 5 Cliquez sur **Suivant**.
- 6 Sur la page Type d'installation, sélectionnez **Installation personnalisée**.
- 7 Dans la section Composant sur la page Type d'installation, sélectionnez **Serveur IaaS**.
- 8 Acceptez l'emplacement d'installation racine ou cliquez sur **Modifier** et sélectionnez le chemin d'installation.
 Même dans un déploiement distribué, vous pouvez être amené à installer plusieurs composants IaaS sur un même serveur Windows.
 Si vous installez plusieurs composants IaaS, veuillez toujours à les installer au même endroit.
- 9 Cliquez sur **Suivant**.
- 10 Sur la page d'installation personnalisée du serveur IaaS, sélectionnez **Base de données**.
- 11 Dans la zone de texte **Instance de base de données**, spécifiez l'instance de base de données ou cliquez sur **Rechercher** et sélectionnez-la dans la liste des instances. Si l'instance de base de données n'est pas un port par défaut, incluez le numéro du port dans la spécification de l'instance en utilisant le formulaire `dbhost,SQL_port_number\SQLinstance`. Le numéro de port par défaut Microsoft SQL est 1443.
- 12 (Facultatif) Cochez la case **Utiliser SSL pour la connexion à la base de données**.
 Par défaut, la case est activée. SSL fournit une connexion plus sécurisée entre le serveur IaaS et la base de données SQL. Néanmoins, vous devez d'abord configurer le protocole SSL sur le serveur SQL pour prendre en charge cette option. Pour obtenir plus d'informations sur la configuration de SSL sur SQL Server, consultez [Article 189067 de Microsoft Technet](#).

13 Sélectionnez le type d'installation de base de données dans le volet **Nom de la base de données**.

- Pour créer le schéma dans une base de données existante, sélectionnez **Utiliser une base de données vide existante**.
- Pour créer une nouvelle base de données, saisissez un nouveau nom de base de données ou utilisez le nom par défaut **vra**. Les noms de base de données ne doivent pas contenir plus de 128 caractères ASCII.

14 Pour spécifier d'autres emplacements, décochez l'option **Utiliser les répertoires de données et de journaux par défaut** ou laissez cette option sélectionnée pour utiliser les répertoires par défaut (recommandé).

15 Sélectionnez le mode d'authentification pour l'installation de la base de données dans la liste **Authentification**.

- Pour utiliser les informations d'identification avec lesquelles vous exécutez le programme d'installation pour créer la base de données, sélectionnez **Utiliser identité Windows...**
- Pour utiliser l'authentification SQL, décochez l'option **Utiliser identité Windows...** Entrez les informations d'identification SQL dans les zones de texte Utilisateur et Mot de passe.

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

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

16 Cliquez sur **Suivant**.

17 Terminez la vérification des conditions préalables.

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

18 Cliquez sur **Installer**.

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

20 Cliquez sur **Terminer**.

Résultats

La base de données est prête à être utilisée.

Installer un composant de site Web IaaS et Model Manager Data

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

Conditions préalables

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

Procédure

1 Installer le premier composant de serveur Web IaaS

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

2 Configurer Model Manager Data

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

Résultats

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

Installer le premier composant de serveur Web IaaS

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

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

Conditions préalables

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

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

Procédure

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

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

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

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

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

Si vous installez plusieurs composants IaaS, veuillez toujours à les installer au même endroit.
- 10 Cliquez sur **Suivant**.
- 11 Sélectionnez **Site Web** et **Données Model Manager** sur la page **Installation personnalisée du serveur IaaS**.
- 12 Sélectionnez un site Web parmi ceux qui sont disponibles ou acceptez le site Web par défaut dans l'onglet **Site Web Administration et Model Manager**.

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

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

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

Il s'agit d'une option moins sécurisée.

Configurer Model Manager Data

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

Conditions préalables

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

Procédure

- 1** Cliquez sur l'onglet **Model Manager Data**.
- 2** Dans la zone de texte **Serveur**, entrez le nom de domaine complet du dispositif vRealize Automation.

vrealize-automation-appliance.mycompany.com

N'entrez pas d'adresse IP.

- 3** Cliquez sur **Charger** pour afficher le **Locataire SSO par défaut**.

Le locataire par défaut `vsphere.local` est créé automatiquement lorsque vous configurez single sign-on. Ne le modifiez pas.

- 4 Cliquez sur **Télécharger** pour importer le certificat à partir du dispositif virtuel.
Le téléchargement du certificat peut prendre quelques minutes.
- 5 (Facultatif) Cliquez sur **Afficher le certificat**, affichez le certificat et cliquez sur **OK** pour fermer la fenêtre d'information.
- 6 Cliquez sur **Accepter le certificat**.
- 7 Entrez **administrator@vsphere.local** dans la zone de texte **Nom d'utilisateur** et entrez le mot de passe que vous avez créé lorsque vous avez configuré SSO dans les zones de texte **Mot de passe** et **Confirmer**.
- 8 (Facultatif) Cliquez sur **Tester** pour vérifier les informations d'identification.
- 9 Dans la zone de texte **Serveur IaaS**, identifiez le composant de serveur Web IaaS.

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

Le port par défaut est 443.

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

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

- 13 Sur la page Paramètres de serveur et de compte, dans les zones de texte **Informations d'installation du serveur**, entrez le nom d'utilisateur et le mot de passe de l'utilisateur du compte de service ayant des privilèges administratifs sur le serveur d'installation actuel.
L'utilisateur du compte de service doit correspondre à un compte de domaine ayant des privilèges sur chaque serveur IaaS distribué. N'utilisez pas de comptes système locaux.

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

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

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

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

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

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

Étape suivante

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

Installer des composants de serveur Web IaaS supplémentaires

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

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

Conditions préalables

- [Installer un composant de site Web IaaS et Model Manager Data](#).
- Vérifiez que le nouveau serveur répond aux exigences dans la section [Serveurs Windows IaaS](#).
- Utilisez l'interface de gestion de dispositif vRealize Automation pour remplacer le certificat afin d'inclure le nom de domaine complet du nouveau nœud. Reportez-vous à [Remplacer les certificats dans le dispositif vRealize Automation](#).

- Si vous avez installé déjà d'autres composants IaaS, vous devez connaître la phrase secrète de la base de données que vous avez créée.
- Si vous utilisez des équilibrages de charge dans votre environnement, vérifiez qu'ils correspondent aux exigences de configuration.

Procédure

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

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

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

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

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

Si vous installez plusieurs composants IaaS, veuillez toujours à les installer au même endroit.
- 10 Cliquez sur **Suivant**.
- 11 Sélectionnez **Site Web** sur la page **Installation personnalisée du serveur IaaS**.

- 12 Sélectionnez un site Web parmi ceux qui sont disponibles ou acceptez le site Web par défaut dans l'onglet **Site Web Administration et Model Manager**.
- 13 Entrez un numéro de port disponible dans la zone de texte **Numéro de port** ou acceptez le port par défaut 443.
- 14 Cliquez sur **Tester la liaison** pour confirmer que le numéro de port est disponible.
- 15 Sélectionnez le certificat pour ce composant.

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

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

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

Il s'agit d'une option moins sécurisée.

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

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

Le port par défaut est 443.

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

21 Terminez la vérification des conditions préalables.

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

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

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

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

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

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

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

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

25 Cliquez sur **Suivant**.**26** Cliquez sur **Installer**.**27** Lorsque l'installation est terminée, désélectionnez **Me guider tout au long de la configuration initiale** et cliquez sur **Suivant**.

Étape suivante

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

Installer le service Active Manager Service

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

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

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

Conditions préalables

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

Procédure

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

En outre, désactivez les contrôles de santé de l'équilibrage de charge jusqu'à ce que tous les composants vRealize Automation aient été installés et configurés.
- 2 Cliquez avec le bouton droit sur le fichier d'installation `setup__vrealize-automation-appliance-FQDN@5480.exe` et sélectionnez **Exécuter en tant qu'administrateur**.
- 3 Acceptez le contrat de licence, puis cliquez sur **Suivant**.

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

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

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

- b Sélectionnez **Accepter le certificat**.

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

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

- 5 Cliquez sur **Suivant**.

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

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

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

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

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

- 9 Cliquez sur **Suivant**.

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

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

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

Le port par défaut est 443.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Étape suivante

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

Installer un composant de sauvegarde Manager Service

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

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

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

Conditions préalables

- Si vous avez installé déjà d'autres composants IaaS, vous devez connaître la phrase secrète de la base de données que vous avez créée.
- (Facultatif) Si vous souhaitez installer Manager Service sur un autre site Web que le site Web par défaut, créez au préalable un site Web dans Internet Information Services.
- Utilisez l'interface de gestion de dispositif vRealize Automation pour remplacer le certificat afin d'inclure le nom de domaine complet du nouveau nœud. Reportez-vous à [Remplacer les certificats dans le dispositif vRealize Automation](#).

- Vérifiez que vous disposez d'un certificat d'une autorité de certification importé dans IIS et que le certificat racine ou l'autorité de certification est approuvé(e). Tous les composants sous l'équilibrage de charge doivent avoir le même certificat.
- Vérifiez que l'équilibrage de charge du site Web est configuré.
- [Installer un composant de site Web IaaS et Model Manager Data.](#)

Procédure

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

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

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

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

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

Si vous installez plusieurs composants IaaS, veuillez toujours à les installer au même endroit.
- 10 Cliquez sur **Suivant**.
- 11 Sélectionnez **Manager Service** sur la page **Installation personnalisée du serveur IaaS**.

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

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

Le port par défaut est 443.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Étape suivante

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

Installation des composants Distributed Execution Manager

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

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

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

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

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

Installer les instances Distributed Execution Manager

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

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

Conditions préalables

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

Procédure

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

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

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

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

- b Sélectionnez **Accepter le certificat**.

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

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

- 5 Cliquez sur **Suivant**.

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

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

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

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

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

- 9 Cliquez sur **Suivant**.

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

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

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

- 12 Cliquez sur **Suivant**.

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

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

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

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

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

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

Le port par défaut est 443.

17 (Facultatif) Cliquez sur **Tester** pour tester les connexions aux services Manager Service et Model Manager Web Service.**18** Cliquez sur **Ajouter**.**19** Cliquez sur **Suivant**.**20** Cliquez sur **Installer**.**21** Lorsque l'installation est terminée, désélectionnez **Me guider tout au long de la configuration initiale** et cliquez sur **Suivant**.**22** Cliquez sur **Terminer**.**Étape suivante**

- Vérifiez que le service est en cours d'exécution et que le journal ne présente aucune erreur. Le nom du service est VMware DEM *Role - Name*, où le rôle est Orchestrator ou Travailleur. L'emplacement du journal est *Install Location\Distributed Execution Manager\Name\Logs*.
- Répétez cette procédure pour installer des instances DEM supplémentaires.

Configurer DEM pour se connecter à SCVMM sur un chemin d'installation différent
Par défaut, le fichier de configuration de DEM Worker utilise le chemin d'installation par défaut de la console de Microsoft System Center Virtual Machine Manager (SCVMM). Si vous installez la console SCVMM dans un emplacement autre que celui par défaut, vous devez mettre à jour le fichier.

Vous avez besoin de cette procédure uniquement si vous avez des points de terminaison et des agents SCVMM.

Conditions préalables

- Souvenez-vous du chemin d'accès par défaut dans lequel vous avez installé la console SCVMM.

Le chemin suivant est le chemin par défaut que vous devez remplacer dans le fichier de configuration.

```
path="{ProgramFiles}\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"
```

Procédure

- 1 Arrêtez le service DEM Worker.
- 2 Ouvrez le fichier suivant dans un éditeur de texte.

Program Files (x86)\VMware\VCAC\Distributed Execution Manager*instance-name*\DynamicOps.DEM.exe.config
- 3 Localisez la section <assemblyLoadConfiguration>.
- 4 Mettez à jour chaque chemin, en utilisant l'exemple suivant comme guide.

```
<assemblyLoadConfiguration>
  <assemblies>
    <!-- List of required assemblies for Scvmm -->
    <add name="Errors" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
    <add name="Microsoft.SystemCenter.VirtualMachineManager" path="D:\Microsoft System Center 2012
R2\Virtual Machine Manager\bin"/>
    <add name="Remoting" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
    <add name="TraceWrapper" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager
\bin"/>
    <add name="Utils" path="D:\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"/>
  </assemblies>
</assemblyLoadConfiguration>
```

- 5 Enregistrez et fermez DynamicOps.DEM.exe.config.
- 6 Redémarrez le service DEM Worker.

Résultats

Pour plus d'informations, reportez-vous à [DEM Workers avec SCVMM](#).

Des informations supplémentaires sur la préparation de l'environnement SCVMM et la création d'un point de terminaison SCVMM sont disponibles dans les documents [Préparation de votre environnement SCVMM](#) et [Créer un point de terminaison Hyper-V \(SCVMM\)](#).

Configuration du service Windows pour accéder à la base de données laaS

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

Windows du compte actuellement connecté est utilisée pour connecter la base de données une fois son installation terminée.

Activez l'accès à la base de données 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.

Conditions préalables

- Choisir un scénario de base de données IaaS.
- Vérifiez que le nom d'utilisateur avec lequel Manager Service doit s'exécuter est défini comme propriétaire de la base de données.

Procédure

- 1 Accédez au sous-répertoire Base de données situé dans le répertoire où vous avez extrait le fichier d'installation compressé (zip).
- 2 Extrayez l'archive DBInstall.zip dans un répertoire local.
- 3 Connectez-vous à l'hôte de la base de données en tant qu'utilisateur avec le rôle **sysadmin** dans l'instance SQL Server.
- 4 Modifiez VMPSOpsUser.sql et remplacez toutes les instances de \$(Service User) par l'utilisateur (à l'étape 3) avec lequel Manager Service doit s'exécuter.

Ne remplacez pas ServiceUser dans la ligne se terminant par WHERE name = N'ServiceUser').
- 5 Ouvrez SQL Server Management Studio.
- 6 Sélectionnez la base de données (vCAC par défaut) dans **Bases de données** dans le volet gauche.
- 7 Cliquez sur **Nouvelle requête**.

La fenêtre Requête SQL s'ouvre dans le volet droit.
- 8 Collez tout le contenu modifié de VMPSOpsUser.sql dans la fenêtre de la requête.
- 9 Cliquez sur **Exécuter**.

Résultats

L'accès à la base de données est activé depuis Manager Service.

Configurer le compte des services Windows pour utiliser l'authentification SQL

Par défaut, le compte des services Windows accède à la base de données lors de l'exécution, même si vous avez configuré la base de données pour l'authentification SQL. Vous pouvez modifier l'authentification au moment de l'exécution de l'authentification Windows à l'authentification SQL.

Il convient notamment de modifier l'authentification au moment de l'exécution lorsque la base de données se trouve dans un domaine non approuvé.

Conditions préalables

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

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](#).

Définir la stratégie d'exécution PowerShell sur RemoteSigned

Vous devez définir la stratégie d'exécution de PowerShell de Restricted à RemoteSigned ou Unrestricted pour permettre aux scripts PowerShell locaux de s'exécuter.

Pour en savoir plus sur la stratégie d'exécution de PowerShell, consultez l'[Article Microsoft PowerShell sur les stratégies d'exécution](#). Si votre stratégie d'exécution PowerShell est gérée au niveau de la stratégie de groupe, contactez votre service d'assistance informatique à propos de ses restrictions sur les modifications de stratégie, et consultez l'[Article Microsoft PowerShell sur les paramètres de stratégie de groupe](#).

Conditions préalables

- Vérifiez que Microsoft PowerShell est installé sur l'hôte d'installation avant l'installation de l'agent. La version requise dépend du système d'exploitation sur l'hôte d'installation. Reportez-vous à l'aide et à l'assistance Windows.
- Pour plus d'informations sur la stratégie d'exécution PowerShell, exécutez `help about_signing` ou `help Set-ExecutionPolicy` sur l'invite de commande PowerShell.

Procédure

- 1 En utilisant un compte d'administrateur, connectez-vous à la machine hôte IaaS sur laquelle l'agent est installé.
- 2 Sélectionnez **Démarrer > Tous les programmes > Version Windows PowerShell > Windows PowerShell**.
- 3 Pour RemoteSigned, exécutez `Set-ExecutionPolicy RemoteSigned`.
- 4 Pour Unrestricted, exécutez `Set-ExecutionPolicy Unrestricted`.
- 5 Vérifiez que la commande n'a pas entraîné d'erreur.
- 6 Tapez **Exit** à l'invite de commande PowerShell.

Choisir le scénario d'installation de l'agent

Les agents que vous devez installer dépendent des systèmes externes avec lesquels vous souhaitez les intégrer.

Tableau 1-35. 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
Provisionner des machines virtuelles via l'intégration avec un environnement Microsoft Hyper-V Server.	Installation de l'agent Proxy pour Hyper-V ou XenServer
Provisionner des machines virtuelles via l'intégration avec un environnement XenServer.	<ul style="list-style-type: none"> ■ Installation de l'agent Proxy pour Hyper-V ou XenServer ■ Installation de l'agent EPI pour Citrix
Provisionner des machines virtuelles via l'intégration avec un environnement XenDesktop.	<ul style="list-style-type: none"> ■ Installation de l'agent VDI pour XenDesktop ■ Installation de l'agent EPI pour Citrix

Tableau 1-35. Choisir un scénario d'installation (suite)

Scénario d'intégration	Conditions requises et procédures pour l'agent
Exécutez des scripts Visual Basic en tant qu'étapes supplémentaires dans le processus de provisionnement avant ou après de provisionner une machine, ou lors de l'annulation du provisionnement.	Installation de l'agent EPI pour les scripts Visual Basic
Collecter des données à partir des machines Windows provisionnées, par exemple le statut Active Directory ou le propriétaire d'une machine.	Installation de l'agent WMI pour les demandes WMI à distance
Provisionner des machines virtuelles via l'intégration avec toute autre plate-forme virtuelle prise en charge.	Il n'est pas nécessaire d'installer un agent.

Emplacement et conditions d'installation de l'agent

Un administrateur système installe généralement les agents sur le serveur vRealize Automation qui héberge le composant Manager Service actif.

Si un agent est installé sur un autre hôte, la configuration réseau doit permettre la communication entre l'agent la machine d'installation de Manager Services.

Chaque agent est installé sous un nom unique dans son propre répertoire, `Agents\agentname`, sous le répertoire d'installation de vRealize Automation (généralement `Program Files(x86)\VMware\VCAC`), avec sa configuration stockée dans le fichier `VRMAgent.exe.config` dans ce répertoire.

Installation et configuration de l'agent Proxy pour vSphere

Un administrateur système installe des agents proxy pour communiquer avec des instances du serveur vSphere. Les agents découvrent le travail disponible, récupèrent les informations de l'hôte et font des rapports sur les éléments de travail terminés et autres modifications de l'état de l'hôte.

Conditions requises de l'agent vSphere

Les informations d'identification du point de terminaison vSphere ou les informations d'identification avec lesquelles l'agent s'exécute doivent avoir un accès administratif à l'hôte d'installation. Plusieurs agents vSphere doivent respecter les conditions requises de configuration de vRealize Automation.

Informations d'identification

Lors de la création d'un point de terminaison représentant l'instance de vCenter Server à faire gérer par un agent vSphere, celui-ci peut utiliser les informations d'identification avec lesquelles le service s'exécute pour interagir avec vCenter Server ou spécifier des informations d'identification de point de terminaison distinctes.

Le privilège `VApp.Import` permet de déployer une machine vSphere en utilisant les paramètres importés à partir d'un fichier OVF. Les détails sur ce privilège vSphere sont disponibles dans la [Documentation de vSphere SDK](#). Si vous prévoyez d'utiliser un point de terminaison vSphere pour déployer des machines virtuelles à partir de modèles OVF, vérifiez que vos informations d'identification incluent le privilège vSphere `VApp.Import` dans l'instance de vCenter Server associée au point de terminaison.

Le tableau suivant répertorie les autorisations dont les informations d'identification du point de terminaison vSphere doivent disposer pour gérer une instance de vCenter Server. Ces autorisations doivent être activées pour tous les clusters de vCenter Server et pas uniquement les clusters qui hébergeront des points de terminaison.

Tableau 1-36. Autorisations requises pour que l'agent vSphere gère une instance de vCenter Server

Valeur de l'attribut		Autorisation
Banque de données		Allouer l'espace
		Parcourir la BD
Cluster de banques de données		Configurer un cluster de banques de données
Dossier		Créer l'annuaire
		Supprimer le dossier
Global		Gérer les attributs personnalisés
		Définir un attribut personnalisé
Réseau		Assigner réseau
Autorisations		Modifier autorisation
vApp		Importer
		Configuration de l'application vApp
Ressource		Attribuer une machine virtuelle au pool de ressources
		Migrer la machine virtuelle hors tension
		Migrer la machine virtuelle sous tension
Machine virtuelle	Inventaire	Créer à partir d'un modèle existant
		Créer nouveau
		Déplacer
		Supprimer
	Interaction	Configurer les supports CD
		Interaction de console
		Connexion de périphérique

Tableau 1-36. Autorisations requises pour que l'agent vSphere gère une instance de vCenter Server (suite)

Valeur de l'attribut	Autorisation
	Mettre hors tension
	Mettre sous tension
	Réinitialiser
	Interrompre
	Installation d'outils
Configuration	Ajouter un disque existant
	Ajouter un nouveau disque
	Ajouter ou supprimer un périphérique
	Supprimer un disque
	Avancé
	Changer le nombre de CPU
	Changer la ressource
	Développer un disque virtuel
	Suivi des changements de disques
	Mémoire
	Modifier les paramètres de périphérique
	Renommer
	Définir une annotation (version 5.0 et ultérieure)
	Paramètres
	Emplacement du fichier d'échange
Provisionnement	Personnaliser
	Modèle de clone
	Cloner machine virtuelle
	Déployer modèle
	Lire les spécifications de personnalisation
État	Créer un snapshot

Tableau 1-36. Autorisations requises pour que l'agent vSphere gère une instance de vCenter Server (suite)

Valeur de l'attribut	Autorisation
	Supprimer le snapshot
	Restaurer le snapshot

Désactivez ou reconfigurez les logiciels tiers susceptibles de modifier l'état de l'alimentation des machines virtuelles situées à l'extérieur de vRealize Automation. Ces modifications peuvent interférer avec la gestion du cycle de vie de la machine par vRealize Automation.

Installer l'agent vSphere

Installez un agent vSphere pour gérer les instances vCenter Server. Pour la haute disponibilité, vous pouvez installer un second agent vSphere redondant pour la même instance vCenter Server. Vous devez nommer et configurer les deux agents vSphere de manière identique, et les installer sur des machines différentes.

Conditions préalables

- Installez IaaS, y compris le serveur Web et l'hôte Manager Service.
- Vérifiez que la machine sur laquelle vous installez l'agent se trouve sur un domaine approuvé par le domaine où les composants IaaS sont installés.
- Vérifiez que la configuration requise dans [Conditions requises de l'agent vSphere](#) est respectée.
- Si vous avez déjà créé un point de terminaison vSphere qui sera utilisé avec cet agent, notez son nom.
- [Télécharger le programme d'installation de vRealize AutomationIaaS](#).

Procédure

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

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

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

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

- b Sélectionnez **Accepter le certificat**.

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

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

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

- 6 Dans la zone Sélection du composant, sélectionnez **Agents proxy**.

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

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

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

- 8 Cliquez sur **Suivant**.

- 9 Connectez-vous avec des privilèges d'administrateur pour les services Windows sur la machine d'installation.

Le service doit être exécuté sur la même machine d'installation.

- 10 Cliquez sur **Suivant**.

- 11 Sélectionnez vSphere dans la liste **Type d'agent**.

- 12 Entrez un identifiant pour cet agent dans la zone de texte **Nom de l'agent**.

Conservez le nom de l'agent, les informations d'identification, le nom du point de terminaison et l'instance de plate-forme pour chaque agent. Vous aurez besoin de ces informations pour configurer les points de terminaison et pour ajouter des hôtes par la suite.

Important Pour la haute disponibilité, vous pouvez ajouter des agents redondants et les configurer de manière identique. Sinon, conservez les agents uniques.

Option	Description
Agent redondant	Installez les agents redondants sur des serveurs distincts. Nommez et configurez les agents redondants de manière identique.
Agent autonome	Attribuez un nom unique à l'agent.

13 Configurez une connexion à l'hôte d'IaaS Manager Service.

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

Le port par défaut est 443.

14 Configurez une connexion au serveur Web IaaS.

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

Le port par défaut est 443.

15 Cliquez sur **Tester** pour vérifier la connectivité avec chaque hôte.**16** Entrez le nom du point de terminaison.

Pour que le point de terminaison fonctionne, le nom que vous configurez dans vRealize Automation doit correspondre au nom du point de terminaison fourni à l'agent proxy vSphere lors de l'installation.

17 Cliquez sur **Ajouter**.**18** Cliquez sur **Suivant**.**19** Cliquez sur **Installer** pour lancer l'installation.

Au bout de quelques minutes, un message de réussite s'affiche.

20 Cliquez sur **Suivant**.**21** Cliquez sur **Terminer**.**22** Vérifiez si l'installation a été effectuée correctement.**23** (Facultatif) Ajoutez plusieurs agents avec des configurations différentes et un point de terminaison sur le même système.

Étape suivante

Configurer l'agent vSphere.

Configurer l'agent vSphere

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

Vous employez l'utilitaire de l'agent proxy pour modifier des parties chiffrées du fichier de configuration de l'agent ou pour modifier la stratégie de suppression de machines pour les plates-formes de virtualisation. Seule une partie du fichier de configuration de l'agent VRMAgent.exe.config est chiffrée. Par exemple, la section serviceConfiguration n'est pas chiffrée.

Conditions préalables

En utilisant un compte avec privilèges d'administrateur, connectez-vous au serveur IaaS Windows sur lequel vous avez installé l'agent vSphere.

Procédure

- 1 Ouvrez une invite de commandes Windows en tant qu'administrateur.
- 2 Passez au dossier d'installation de l'agent, où *agent-name* est le dossier contenant l'agent vSphere.

```
cd %SystemDrive%\Program Files (x86)\VMware\VCAC\Agents\agent-name
```

- 3 (Facultatif) Pour afficher les paramètres de configuration actuels, entrez la commande suivante.

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config get
```

Voici un exemple de sortie de la commande.

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

- 4 (Facultatif) Pour modifier le nom du point de terminaison que vous avez configuré lors de l'installation, utilisez la commande suivante.

```
set managementEndpointName
```

Par exemple : `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set managementEndpointName my-endpoint`

Vous utilisez ce processus pour renommer le point de terminaison dans vRealize Automation plutôt que de modifier les points de terminaison.

- 5 (Facultatif) Pour configurer la stratégie de suppression de machines virtuelles, utilisez la commande suivante.

```
set doDeletes
```

Par exemple : `DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set doDeletes false`

Option	Description
true	(Par défaut) Supprimer les machines virtuelles détruites dans vRealize Automation depuis vCenter Server.
false	Déplacez les machines virtuelles détruites dans vRealize Automation vers le répertoire VRMDelated dans vCenter Server.

- Ouvrez **Outils d'administration > Services** et redémarrez le service vRealize Automation Agent – *agent-name*.

Étape suivante

Pour la haute disponibilité, vous pouvez installer et configurer un agent redondant pour votre point de terminaison. Installez chaque agent redondant sur un serveur distinct, mais nommez et configurez les agents de manière identique.

Installation de l'agent Proxy pour Hyper-V ou XenServer

Un administrateur système installe des agents proxy pour communiquer avec des instances du serveur Hyper-V ou XenServer. Les agents découvrent le travail disponible, récupèrent les informations de l'hôte et font des rapports sur les éléments de travail terminés et autres modifications de l'état de l'hôte.

Conditions requises pour Hyper-V et XenServer

Les agents proxy Hyper-V Hypervisor requièrent des informations d'identification pour l'installation.

Les informations d'identification avec lesquelles l'agent de service est exécuté doivent disposer d'un accès d'administration à l'hôte d'installation.

Des informations d'identification de niveau administrateur sont requises pour toutes les instances XenServer ou Hyper-V sur les hôtes qui doivent être gérés par l'agent.

Si vous utilisez des pools Xen, tous les nœuds qu'ils contiennent doivent être identifiés par leurs noms de domaines complets.

Note Par défaut, Hyper-V n'est pas configuré pour la gestion à distance. Un agent proxy vRealize AutomationHyper-V ne peut pas communiquer avec un serveur Hyper-V si la gestion à distance n'a pas été activée.

Pour obtenir des informations sur la procédure de configuration de Hyper-V pour la gestion à distance, reportez-vous à la documentation Microsoft Windows Server.

Installer l'agent Hyper-V ou XenServer

L'agent Hyper-V gère les instances de serveur Hyper-V. L'agent XenServer gère les instances de serveur XenServer.

Conditions préalables

- Installez IaaS, y compris le serveur Web et l'hôte Manager Service.

- [Télécharger le programme d'installation de vRealize AutomationIaaS](#).
- Vérifiez que les agents proxy de l'hyperviseur Hyper-V ont les mêmes informations d'identification d'administrateur système.
- Vérifiez que les informations d'identification avec lesquelles le service d'agent est exécuté ont des droits d'accès d'administration à l'hôte d'installation.
- Vérifiez que toutes les instances XenServer ou Hyper-V sur les hôtes qui doivent être gérés par l'agent ont des informations d'identification du niveau administrateur.
- Si vous utilisez des pools Xen, notez que tous les nœuds au sein du pool Xen doivent être identifiés par leurs noms de domaine complets.

vRealize Automation ne peut pas gérer ni communiquer avec les nœuds qui ne sont pas identifiés par leur nom de domaine complet au sein du pool Xen.

- Configurez Hyper-V pour la gestion à distance afin de permettre la communication du serveur Hyper-V avec les agents proxy vRealize AutomationHyper-V.

Pour obtenir des informations sur la procédure de configuration de Hyper-V pour la gestion à distance, reportez-vous à la documentation Microsoft Windows Server.

Procédure

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

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

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

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

- 8** Cliquez sur **Suivant**.

- 9** Connectez-vous avec des privilèges d'administrateur pour les services Windows sur la machine d'installation.

Le service doit être exécuté sur la même machine d'installation.

- 10** Cliquez sur **Suivant**.

- 11** Sélectionnez l'agent dans la liste **Type d'agent**.

- Xen
- Hyper-V

- 12** Entrez un identifiant pour cet agent dans la zone de texte **Nom de l'agent**.

Conservez le nom de l'agent, les informations d'identification, le nom du point de terminaison et l'instance de plate-forme pour chaque agent. Vous aurez besoin de ces informations pour configurer les points de terminaison et pour ajouter des hôtes par la suite.

Important Pour la haute disponibilité, vous pouvez ajouter des agents redondants et les configurer de manière identique. Sinon, conservez les agents uniques.

Option	Description
Agent redondant	Installez les agents redondants sur des serveurs distincts. Nommez et configurez les agents redondants de manière identique.
Agent autonome	Attribuez un nom unique à l'agent.

- 13** Communiquez le **Nom de l'agent** à l'administrateur IaaS qui configure les points de terminaison.

Pour permettre l'accès et la collecte des données, le point de terminaison doit être lié à l'agent qui a été configuré pour lui.

14 Configurez une connexion à l'hôte d'IaaS Manager Service.

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

Le port par défaut est 443.

15 Configurez une connexion au serveur Web IaaS.

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

Le port par défaut est 443.

16 Cliquez sur **Tester** pour vérifier la connectivité avec chaque hôte.**17** Entrez les informations d'identification d'un utilisateur avec des autorisations de niveau administrateur sur l'instance de serveur géré.**18** Cliquez sur **Ajouter**.**19** Cliquez sur **Suivant**.**20** (Facultatif) Ajoutez un autre agent.

Par exemple, vous pouvez ajouter un agent Xen si vous avez précédemment ajouté l'agent Hyper-V.

21 Cliquez sur **Installer** pour lancer l'installation.

Au bout de quelques minutes, un message de réussite s'affiche.

22 Cliquez sur **Suivant**.**23** Cliquez sur **Terminer**.**24** Vérifiez si l'installation a été effectuée correctement.

Étape suivante

Pour la haute disponibilité, vous pouvez installer et configurer un agent redondant pour votre point de terminaison. Installez chaque agent redondant sur un serveur distinct, mais nommez et configurez les agents de manière identique.

[Configurer l'agent Hyper-V ou XenServer.](#)

Configurer l'agent Hyper-V ou XenServer

Un administrateur système peut modifier les paramètres de configuration de l'agent proxy, par exemple la stratégie de suppression des plates-formes de virtualisation. Vous pouvez utiliser l'utilitaire de l'agent proxy pour modifier les configurations initiales qui sont chiffrées dans le fichier de configuration de l'agent.

Conditions préalables

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

Procédure

- 1 Passez au répertoire d'installation des agents, où *agent_name* est le répertoire qui contient l'agent proxy et qui est également le nom sous lequel l'agent est installé.

```
cd Program Files (x86)\VMware\VCAC Agents\agent_name
```

- 2 Afficher les paramètres de configuration actuels.

```
Entrez DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config get
```

Voici un exemple de sortie de commande :

```
Username: XSadmin
```

- 3 Entrez la commande set pour modifier une propriété, où *propriété* est l'une des options affichée dans le tableau.

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set la valeur de la propriété
```

Si vous omettez la *valeur*, l'utilitaire vous invite à renseigner une nouvelle valeur.

Propriété	Description
username	Le nom d'utilisateur représentant les informations d'identification de niveau administrateur pour le serveur XenServer ou Hyper-V avec lequel l'agent communique.
password	Le mot de passe pour le nom d'utilisateur de niveau administrateur.

- 4 Cliquez sur **Démarrer > Outils d'administration > Services**, puis redémarrez le service vRealize Automation Agent – *nom de l'agent*.

Exemple : Modifier les informations d'identification de niveau administrateur

Entrez la commande suivante pour modifier les informations d'identification de niveau administrateur pour la plate-forme de virtualisation spécifiée lors de l'installation de l'agent.

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set username jsmith
```

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set password
```

Étape suivante

Pour la haute disponibilité, vous pouvez installer et configurer un agent redondant pour votre point de terminaison. Installez chaque agent redondant sur un serveur distinct, mais nommez et configurez les agents de manière identique.

Installation de l'agent VDI pour XenDesktop

vRealize Automation utilise des agents VDI PowerShell pour enregistrer les machines XenDesktop qu'il provisionne auprès de systèmes de gestion de bureau externes.

L'agent d'intégration VDI fournit aux propriétaires de machines enregistrées une connexion directe à l'interface Web XenDesktop. Vous pouvez installer un agent en tant qu'agent dédié à l'interaction avec un seul DDC (Desktop Delivery Controller) ou en tant qu'agent général pouvant interagir avec plusieurs DDC.

Conditions requises de XenDesktop

Un administrateur système installe un agent VDI pour intégrer des serveurs XenDesktop à vRealize Automation.

Vous pouvez installer un agent VDI général pour interagir avec plusieurs serveurs. Si vous installez un agent dédié par serveur pour l'équilibrage de charge ou des motifs d'autorisation, vous devez fournir le nom du serveur DDC XenDesktop lors de l'installation de l'agent. Un agent dédié peut gérer uniquement les demandes d'enregistrement adressées au serveur spécifiées dans sa configuration.

Pour plus d'informations sur les versions prises en charge de XenDesktop pour les serveurs DDC XenDesktop, reportez-vous à la *Matrice de prise en charge de vRealize Automation* sur le site Web de VMware.

Hôte et informations d'identification d'installation

Les informations d'identification avec lesquelles l'agent s'exécute doivent disposer d'un accès administratif à tous les serveurs DDC XenDesktop avec lesquels il interagit.

Conditions requises de XenDesktop

Le nom attribué à l'hôte XenServer sur votre serveur XenDesktop doit correspondre à l'UUID du pool de serveurs Xen dans XenCenter. Consultez [Définir le nom d'hôte XenServer](#) pour plus d'informations.

Chaque serveur DDC XenDesktop auprès duquel vous comptez enregistrer des machines doit être configuré comme suit :

- Le type du groupe/catalogue doit être défini sur **Existant** pour être utilisé avec vRealize Automation.
- Le nom d'un hôte vCenter Server sur un serveur DDC doit correspondre au nom de l'instance de vCenter Server entré dans le point de terminaison vSphere vRealize Automation, sans le domaine. Le point de terminaison doit être configuré avec un nom de domaine complet et non avec une adresse IP. Par exemple, si l'adresse dans le point de terminaison est `https://virtual-center27.domain/sdk`, le nom de l'hôte sur le serveur DDC doit être défini sur `virtual-center27`.

Si votre point de terminaison vSphere vRealize Automation a été configuré avec une adresse IP, vous devez le modifier pour utiliser un nom de domaine complet. Pour plus d'informations sur la configuration des points de terminaison, reportez-vous à la documentation *Configuration d'IaaS*.

Conditions requises de l'hôte de l'agent XenDesktop

Citrix XenDesktop SDK doit être installé. Le SDK pour XenDesktop est inclus dans le disque d'installation de XenDesktop.

Vérifiez que Microsoft PowerShell est installé sur l'hôte d'installation avant l'installation de l'agent. La version requise dépend du système d'exploitation sur l'hôte d'installation. Reportez-vous à l'aide et à l'assistance Windows.

La stratégie d'exécution MS PowerShell est définie sur RemoteSigned ou Unrestricted. Reportez-vous à [Définir la stratégie d'exécution PowerShell sur RemoteSigned](#).

Pour plus d'informations sur la stratégie d'exécution PowerShell, exécutez `help about_signing` ou `help Set-ExecutionPolicy` sur l'invite de commande PowerShell.

Définir le nom d'hôte XenServer

Dans XenDesktop, le nom attribué à l'hôte XenServer sur votre serveur XenDesktop doit correspondre à l'UUID du pool de serveurs Xen dans XenCenter. Si aucun XenPool n'est configuré, le nom doit correspondre à l'UUID de l'hôte XenServer lui-même.

Procédure

- 1 Dans Citrix XenCenter, sélectionnez votre XenPool ou XenServer autonome et cliquez sur l'onglet **Général**. Enregistrez l'UUID.
- 2 Lorsque vous ajoutez votre pool de serveurs XenServer ou votre hôte autonome à XenDesktop, tapez l'UUID enregistré à l'étape précédente en tant que nom de la **Connexion**.

Installer l'agent XenDesktop

Les agents PowerShell d'intégration de bureau virtuel (VDI) s'intègrent au système de bureaux virtuels externe, comme XenDesktop et Citrix. Utilisez un agent PowerShell VDI pour gérer la machine XenDesktop.

Conditions préalables

- Installez IaaS, y compris le serveur Web et l'hôte Manager Service.
- Vérifiez que la configuration requise dans [Conditions requises de XenDesktop](#) est respectée.
- [Télécharger le programme d'installation de vRealize Automation IaaS](#).

Procédure

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

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

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

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

Si vous installez plusieurs composants IaaS, veuillez toujours à les installer au même endroit.
- 9 Cliquez sur **Suivant**.
- 10 Connectez-vous avec des privilèges d'administrateur pour les services Windows sur la machine d'installation.

Le service doit être exécuté sur la même machine d'installation.
- 11 Cliquez sur **Suivant**.
- 12 Sélectionnez **PowerShell VDI** dans la liste **Type d'agent**.

13 Entrez un identifiant pour cet agent dans la zone de texte **Nom de l'agent**.

Conservez le nom de l'agent, les informations d'identification, le nom du point de terminaison et l'instance de plate-forme pour chaque agent. Vous aurez besoin de ces informations pour configurer les points de terminaison et pour ajouter des hôtes par la suite.

Important Pour la haute disponibilité, vous pouvez ajouter des agents redondants et les configurer de manière identique. Sinon, conservez les agents uniques.

Option	Description
Agent redondant	Installez les agents redondants sur des serveurs distincts. Nommez et configurez les agents redondants de manière identique.
Agent autonome	Attribuez un nom unique à l'agent.

14 Configurez une connexion à l'hôte d'IaaS Manager Service.

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

Le port par défaut est 443.

15 Configurez une connexion au serveur Web IaaS.

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

Le port par défaut est 443.

16 Cliquez sur **Tester** pour vérifier la connectivité avec chaque hôte.**17** Sélectionnez la **Version de VDI**.**18** Entrez le nom de domaine complet du serveur géré dans la zone de texte **Serveur VDI**.**19** Cliquez sur **Ajouter**.

20 Cliquez sur **Suivant**.

21 Cliquez sur **Installer** pour lancer l'installation.

Au bout de quelques minutes, un message de réussite s'affiche.

22 Cliquez sur **Suivant**.

23 Cliquez sur **Terminer**.

24 Vérifiez si l'installation a été effectuée correctement.

25 (Facultatif) Ajoutez plusieurs agents avec des configurations différentes et un point de terminaison sur le même système.

Étape suivante

Pour la haute disponibilité, vous pouvez installer et configurer un agent redondant pour votre point de terminaison. Installez chaque agent redondant sur un serveur distinct, mais nommez et configurez les agents de manière identique.

Installation de l'agent EPI pour Citrix

Les agents EPI PowerShell intègrent des machines externes Citrix au processus de provisionnement. L'agent EPI diffuse à la demande les images du disque Citrix à partir desquelles les machines démarrent et s'exécutent.

L'agent EPI dédié interagit avec un serveur de provisionnement externe unique. Vous devez installer un agent EPI pour chaque instance du serveur de provisionnement Citrix.

Conditions requises pour Citrix Provisioning Server

Un administrateur système utilise des agents External Provisioning Infrastructure (EPI) pour intégrer les serveurs de provisionnement Citrix et pour activer l'utilisation des scripts Visual Basic dans le processus de provisionnement.

Emplacement d'installation et informations d'identification

Installez l'agent sur l'hôte PVS pour les instances de Citrix Provisioning Services. Vérifiez que l'hôte d'installation répond aux [Conditions requises pour l'agent hôte Citrix](#) avant d'installer l'agent.

Même si un agent EPI peut généralement interagir avec plusieurs serveurs, Citrix Provisioning Server requiert un agent EPI dédié. Vous devez installer un agent EPI pour chaque instance de Citrix Provisioning Server, en fournissant le nom du serveur qui l'héberge. Les informations d'identification avec lesquelles l'agent s'exécute doivent avoir un accès administratif à l'instance de Citrix Provisioning Server.

Reportez-vous à *Matrice de prise en charge de vRealize Automation* pour plus d'informations sur les versions de Citrix PVS prises en charge.

Conditions requises pour l'agent hôte Citrix

PowerShell et Citrix Provisioning Services SDK doivent être installés sur l'hôte d'installation avant d'installer l'agent. Pour plus de détails, reportez-vous à *Matrice de prise en charge de vRealize Automation* sur le site Web de VMware.

Vérifiez que Microsoft PowerShell est installé sur l'hôte d'installation avant l'installation de l'agent. La version requise dépend du système d'exploitation sur l'hôte d'installation. Reportez-vous à l'aide et à l'assistance Windows.

Vous devez également vous assurer que le composant logiciel enfichable de PowerShell est installé. Pour plus d'informations, reportez-vous au *Guide du programmeur PowerShell pour Citrix Provisioning Services* sur le site Web de Citrix.

La stratégie d'exécution MS PowerShell est définie sur RemoteSigned ou Unrestricted. Reportez-vous à [Définir la stratégie d'exécution PowerShell sur RemoteSigned](#).

Pour plus d'informations sur la stratégie d'exécution PowerShell, exécutez `help about_signing` ou `help Set-ExecutionPolicy` sur l'invite de commande PowerShell.

Installer l'agent Citrix

Les agents PowerShell d'intégration de provisionnement externe (EPI) intègrent des systèmes externes dans le processus de provisionnement des machines. Utilisez l'agent PowerShell EPI pour l'intégration à un serveur Citrix pour permettre le provisionnement de machines par diffusion à la demande de disque.

Conditions préalables

- Installez IaaS, y compris le serveur Web et l'hôte Manager Service.
- Vérifiez que la configuration requise dans [Conditions requises pour Citrix Provisioning Server](#) est respectée.
- [Télécharger le programme d'installation de vRealize AutomationIaaS](#).

Procédure

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

- 5 Sur la page Type d'installation, sélectionnez **Installation personnalisée**.
- 6 Sélectionnez **Sélection du composant** sur la page Type d'installation.
- 7 Acceptez l'emplacement d'installation racine ou cliquez sur **Modifier** et sélectionnez le chemin d'installation.

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

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

- 8 Cliquez sur **Suivant**.
- 9 Connectez-vous avec des privilèges d'administrateur pour les services Windows sur la machine d'installation.

Le service doit être exécuté sur la même machine d'installation.

- 10 Cliquez sur **Suivant**.
- 11 Dans la liste Type d'agent, sélectionnez **Power Shell EPI**.
- 12 Entrez un identifiant pour cet agent dans la zone de texte **Nom de l'agent**.

Conservez le nom de l'agent, les informations d'identification, le nom du point de terminaison et l'instance de plate-forme pour chaque agent. Vous aurez besoin de ces informations pour configurer les points de terminaison et pour ajouter des hôtes par la suite.

Important Pour la haute disponibilité, vous pouvez ajouter des agents redondants et les configurer de manière identique. Sinon, conservez les agents uniques.

Option	Description
Agent redondant	Installez les agents redondants sur des serveurs distincts. Nommez et configurez les agents redondants de manière identique.
Agent autonome	Attribuez un nom unique à l'agent.

- 13 Configurez une connexion à l'hôte d'IaaS Manager Service.

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

Le port par défaut est 443.

14 Configurez une connexion au serveur Web IaaS.

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

Le port par défaut est 443.

15 Cliquez sur **Tester** pour vérifier la connectivité avec chaque hôte.

16 Sélectionnez le type d'EPI.

17 Entrez le nom de domaine complet du serveur géré dans la zone de texte **Serveur EPI**.

18 Cliquez sur **Ajouter**.

19 Cliquez sur **Suivant**.

20 Cliquez sur **Installer** pour lancer l'installation.

Au bout de quelques minutes, un message de réussite s'affiche.

21 Cliquez sur **Suivant**.

22 Cliquez sur **Terminer**.

23 Vérifiez si l'installation a été effectuée correctement.

24 (Facultatif) Ajoutez plusieurs agents avec des configurations différentes et un point de terminaison sur le même système.

Étape suivante

Pour la haute disponibilité, vous pouvez installer et configurer un agent redondant pour votre point de terminaison. Installez chaque agent redondant sur un serveur distinct, mais nommez et configurez les agents de manière identique.

Installation de l'agent EPI pour les scripts Visual Basic

Un administrateur système peut définir des scripts Visual Basic comme étapes supplémentaires du processus de provisionnement avant ou après le provisionnement d'une machine ou lors de l'annulation du provisionnement d'une machine. Avant d'exécuter des scripts Visual Basic, vous devez installer un EPI PowerShell.

Les scripts Visual Basic sont spécifiés dans le Blueprint à partir duquel les machines sont provisionnées. Ces scripts ont accès à toutes les propriétés personnalisées associées à la machine et peuvent mettre à jour leurs valeurs. L'étape suivante du workflow a ensuite accès à ces nouvelles valeurs.

Vous pouvez, par exemple, utiliser un script pour générer des certificats ou des jetons de sécurité avant le provisionnement afin de les utiliser lors du provisionnement des machines.

Pour autoriser les scripts pendant le provisionnement, vous devez installer un type spécifique d'agent EPI et placer les scripts que vous souhaitez utiliser sur le système sur lequel l'agent est installé.

Lors de l'exécution d'un script, l'agent EPI transmet toutes les propriétés personnalisées de la machine comme arguments au script. Pour renvoyer des valeurs de propriétés mises à jour, vous devez placer ces propriétés dans un dictionnaire et appeler une fonction vRealize Automation. Un exemple de script est inclus dans le sous-répertoire des scripts du répertoire d'installation de l'agent EPI. Ce script contient un en-tête permettant de charger tous les arguments dans un dictionnaire, un corps dans lequel vous pouvez inclure votre ou vos fonctions et un pied de page permettant de renvoyer les valeurs de propriétés personnalisées mises à jour.

Note Vous pouvez installer plusieurs agents EPI/VBScripts sur plusieurs serveurs et effectuer le provisionnement avec un agent spécifique et les scripts Visual Basic de l'hôte de cet agent. Si vous avez besoin d'effectuer cette opération, contactez le support client de VMware.

Conditions requises pour les scripts Visual Basic

Un administrateur système installe des agents EPI pour permettre l'utilisation de scripts Visual Basic au cours du processus de provisionnement.

Le tableau suivant présente les conditions requises s'appliquant pour l'installation d'un agent EPI permettant d'activer l'utilisation de scripts Visual Basic dans le processus de provisionnement.

Tableau 1-37. Agents EPI pour l'écriture de scripts Visual

Conditions requises	Description
Informations d'identification	Les informations d'identification avec lesquelles l'agent s'exécute doit avoir un accès administratif à l'hôte d'installation.
Microsoft PowerShell	Microsoft PowerShell doit être installé sur l'hôte d'installation avant l'installation de l'agent : la version requise dépend du système d'exploitation de l'hôte d'installation et peut avoir été installée avec ce système d'exploitation. Pour plus d'informations, consultez la page http://support.microsoft.com .
Stratégie d'exécution MS PowerShell	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 : <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <pre>help about_signing help Set-ExecutionPolicy</pre> </div>

Installer l'agent pour les scripts Visual Basic

Les agents Power Shell d'intégration de provisionnement externe (EPI) permettent d'intégrer des systèmes externes dans le processus de provisionnement des machines. Utilisez un agent EPI pour exécuter les scripts Visual Basic comme étapes supplémentaires lors du processus de provisionnement.

Conditions préalables

- Installez IaaS, y compris le serveur Web et l'hôte Manager Service.
- Vérifiez que la configuration requise dans [Conditions requises pour les scripts Visual Basic](#) est respectée.
- [Télécharger le programme d'installation de vRealize Automation IaaS](#).

Procédure

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

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

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

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

Si vous installez plusieurs composants IaaS, veillez toujours à les installer au même endroit.
- 8 Cliquez sur **Suivant**.
- 9 Connectez-vous avec des privilèges d'administrateur pour les services Windows sur la machine d'installation.

Le service doit être exécuté sur la même machine d'installation.
- 10 Cliquez sur **Suivant**.
- 11 Dans la liste Type d'agent, sélectionnez **Power Shell EPI**.

12 Entrez un identifiant pour cet agent dans la zone de texte **Nom de l'agent**.

Conservez le nom de l'agent, les informations d'identification, le nom du point de terminaison et l'instance de plate-forme pour chaque agent. Vous aurez besoin de ces informations pour configurer les points de terminaison et pour ajouter des hôtes par la suite.

Important Pour la haute disponibilité, vous pouvez ajouter des agents redondants et les configurer de manière identique. Sinon, conservez les agents uniques.

Option	Description
Agent redondant	Installez les agents redondants sur des serveurs distincts. Nommez et configurez les agents redondants de manière identique.
Agent autonome	Attribuez un nom unique à l'agent.

13 Configurez une connexion à l'hôte d'IaaS Manager Service.

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

Le port par défaut est 443.

14 Configurez une connexion au serveur Web IaaS.

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

Le port par défaut est 443.

15 Cliquez sur **Tester** pour vérifier la connectivité avec chaque hôte.**16** Sélectionnez le type d'EPI.**17** Entrez le nom de domaine complet du serveur géré dans la zone de texte **Serveur EPI**.**18** Cliquez sur **Ajouter**.

19 Cliquez sur **Suivant**.

20 Cliquez sur **Installer** pour lancer l'installation.

Au bout de quelques minutes, un message de réussite s'affiche.

21 Cliquez sur **Suivant**.

22 Cliquez sur **Terminer**.

23 Vérifiez si l'installation a été effectuée correctement.

24 (Facultatif) Ajoutez plusieurs agents avec des configurations différentes et un point de terminaison sur le même système.

Installation de l'agent WMI pour les demandes WMI à distance

Un administrateur système active le protocole WMI et installe l'agent WMI sur toutes les machines Windows gérées pour autoriser la gestion des données et des opérations. L'agent doit collecter des données auprès des machines Windows, comme l'état Active Directory du propriétaire d'une machine.

Activer les demandes WMI à distance sur les machines Windows

Pour utiliser les agents WMI, les demandes WMI à distance doivent être activées sur les serveurs Windows gérés.

Procédure

- 1** Dans chaque domaine contenant des machines virtuelles provisionnées et gérées, créez un groupe Active Directory et ajoutez-le aux informations d'identification du service des agents WMI qui exécutent les demandes WMI à distance sur les machines provisionnées.
- 2** Activez les demandes WMI à distance pour les groupes Active Directory contenant les informations d'identification d'agent sur chaque machine provisionnée Windows.

Installer l'agent WMI

L'agent Windows Management Instrumentation (WMI) permet la collecte des données à partir des machines gérées Windows.

Conditions préalables

- Installez IaaS, y compris le serveur Web et l'hôte Manager Service.
- Vérifiez que la configuration requise dans [Activer les demandes WMI à distance sur les machines Windows](#) est respectée.
- [Télécharger le programme d'installation de vRealize AutomationIaaS](#).

Procédure

- 1** Cliquez avec le bouton droit sur le fichier d'installation `setup__vrealize-automation-appliance-FQDN@5480.exe` et sélectionnez **Exécuter en tant qu'administrateur**.
- 2** Cliquez sur **Suivant**.

- 3 Acceptez le contrat de licence, puis cliquez sur **Suivant**.
- 4 Sur la page de connexion, fournissez les informations d'identification d'administrateur pour le dispositif vRealize Automation et vérifiez le certificat SSL.
 - a Entrez le nom d'utilisateur **root** et le mot de passe.

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

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

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

Si vous installez plusieurs composants IaaS, veuillez toujours à les installer au même endroit.
- 8 Cliquez sur **Suivant**.
- 9 Connectez-vous avec des privilèges d'administrateur pour les services Windows sur la machine d'installation.

Le service doit être exécuté sur la même machine d'installation.
- 10 Cliquez sur **Suivant**.
- 11 Sélectionnez **WMI** dans la liste **Type d'agent**.

12 Entrez un identifiant pour cet agent dans la zone de texte **Nom de l'agent**.

Conservez le nom de l'agent, les informations d'identification, le nom du point de terminaison et l'instance de plate-forme pour chaque agent. Vous aurez besoin de ces informations pour configurer les points de terminaison et pour ajouter des hôtes par la suite.

Important Pour la haute disponibilité, vous pouvez ajouter des agents redondants et les configurer de manière identique. Sinon, conservez les agents uniques.

Option	Description
Agent redondant	Installez les agents redondants sur des serveurs distincts. Nommez et configurez les agents redondants de manière identique.
Agent autonome	Attribuez un nom unique à l'agent.

13 Configurez une connexion à l'hôte d'IaaS Manager Service.

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

Le port par défaut est 443.

14 Configurez une connexion au serveur Web IaaS.

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

Le port par défaut est 443.

15 Cliquez sur **Tester** pour vérifier la connectivité avec chaque hôte.**16** Cliquez sur **Ajouter**.**17** Cliquez sur **Suivant**.

18 Cliquez sur **Installer** pour lancer l'installation.

Au bout de quelques minutes, un message de réussite s'affiche.

19 Cliquez sur **Suivant**.

20 Cliquez sur **Terminer**.

21 Vérifiez si l'installation a été effectuée correctement.

22 (Facultatif) Ajoutez plusieurs agents avec des configurations différentes et un point de terminaison sur le même système.

Installation silencieuse de vRealize Automation

vRealize Automation inclut des options pour l'installation silencieuse basée sur un script à partir de la ligne de commande et l'installation silencieuse basée sur API. Les deux approches imposent que vous prépariez d'avance les valeurs que vous devriez normalement saisir manuellement lors d'une installation classique.

À propos de l'installation silencieuse de vRealize Automation

L'installation silencieuse de vRealize Automation utilise un fichier exécutable qui fait référence à un fichier texte de réponses.

Dans le fichier de réponses, vous préconfigurez les noms de domaine complets du système, les informations d'identification de compte et d'autres paramètres que vous ajoutez généralement tout au long d'une installation traditionnelle basée sur assistant ou manuelle. L'installation silencieuse s'avère utile pour les types de déploiement suivants :

- Déploiement de nombreux environnements quasiment identiques
- Redéploiements répétés du même environnement
- Installations sans assistance
- Installations avec scripts

Effectuer une installation silencieuse de vRealize Automation

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

Conditions préalables

- Créer un dispositif non configuré. Reportez-vous à [Déployer le dispositif vRealize Automation](#).
- Créez ou identifiez vos serveurs Windows IaaS et configurez leurs conditions préalables.
- Installez l'agent de gestion sur vos serveurs Windows IaaS.

Vous pouvez installer l'agent de gestion à l'aide du fichier téléchargé .msi traditionnel ou à l'aide du processus silencieux décrit dans la section [Effectuer une installation silencieuse de l'agent de gestion de vRealize Automation](#).

Procédure

- 1 Connectez-vous à la console du dispositif vRealize Automation en tant qu'utilisateur racine.

- 2 Accédez au répertoire suivant :

```
/usr/lib/vcac/tools/install
```

- 3 Ouvrez le fichier de réponses `ha.properties` dans un éditeur de texte.

- 4 Ajoutez les entrées spécifiques à votre déploiement dans le fichier `ha.properties`, puis enregistrez et fermez le fichier.

Vous pouvez également gagner du temps en copiant et en modifiant un fichier `ha.properties` d'un autre déploiement au lieu de modifier l'ensemble du fichier par défaut.

- 5 Démarrez l'installation à partir du même annuaire en exécutant la commande suivante :

```
vra-ha-config.sh
```

L'installation peut prendre jusqu'à une heure, voire plus, selon l'environnement et la taille du déploiement.

- 6 (Facultatif) Une fois l'installation terminée, examinez le fichier journal :

```
/var/log/vcac/vra-ha-config.log.
```

Le programme d'installation silencieuse n'enregistre pas les données exclusives, telles que les mots de passe, licences ou certificats, dans le journal.

Effectuer une installation silencieuse de l'agent de gestion de vRealize Automation

Vous pouvez effectuer une ligne de commande basée sur l'installation de l'agent de gestion de vRealize Automation sur n'importe quel serveur Windows IaaS.

L'installation silencieuse de l'agent de gestion se compose d'un script Windows PowerShell dont vous personnalisez quelques paramètres. Après avoir ajouté les paramètres spécifiques à votre déploiement, vous pouvez installer silencieusement l'agent de gestion sur tous vos serveurs Windows IaaS en exécutant des copies du même script sur chacun d'eux.

Conditions préalables

- Créer un dispositif non configuré. Reportez-vous à [Déployer le dispositif vRealize Automation](#).
- Créez ou identifiez vos serveurs Windows IaaS et configurez leurs conditions préalables.

Procédure

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

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

- 3 Cliquez avec le bouton droit sur le fichier de script PowerShell `InstallManagementAgent.ps1` et enregistrez-le sur le bureau ou dans un dossier du serveur Windows IaaS.
- 4 Ouvrez `InstallManagementAgent.ps1` dans un éditeur de texte.
- 5 Vers le haut du fichier de script, ajoutez les paramètres spécifiques à votre déploiement.
 - URL du dispositif vRealize Automation
`https://vrealize-automation-appliance-FQDN:5480`
 - Informations d'identification du compte d'utilisateur racine du dispositif vRealize Automation
 - Informations d'identification de l'utilisateur du service vRealize Automation, un compte de domaine avec privilèges d'administrateur sur les serveurs Windows IaaS
 - Dossier dans lequel vous voulez installer l'agent de gestion, Program Files (x86) par défaut
 - (Facultatif) Empreinte numérique du certificat au format PEM que vous utilisez pour l'authentification
- 6 Enregistrez et fermez le fichier `InstallManagementAgent.ps1`.
- 7 Pour installer silencieusement l'agent de gestion, double-cliquez sur `InstallManagementAgent.ps1`.
- 8 (Facultatif) Assurez-vous que l'installation s'est achevée en localisant l'**agent de gestion de VMware vCloud Automation Center** dans la liste Programmes et fonctionnalités du panneau de configuration Windows, et dans la liste des services Windows qui s'exécutent.

Fichier de réponses pour installation silencieuse de vRealize Automation

Les installations silencieuses de vRealize Automation nécessitent la préparation préalable d'un fichier texte de réponses.

Tous les dispositifs vRealize Automation qui viennent d'être déployés contiennent un fichier de réponses par défaut :

`/usr/lib/vcac/tools/install/ha.properties`.

Pour effectuer une installation silencieuse, vous devez utiliser un éditeur de texte pour personnaliser les paramètres du fichier `ha.properties` et adapter ces derniers au déploiement souhaité. Les exemples suivants présentent certains des paramètres et informations que vous devez ajouter.

- Votre clé de licence vRealize Automation ou de suite logicielle
- Noms de domaine complets des nœuds dispositif vRealize Automation
- Informations d'identification du compte d'utilisateur racine de dispositif vRealize Automation
- Noms de domaine complets des serveurs Windows IaaS qui feront office de nœuds Web, de nœuds Manager Service, etc.

- Informations d'identification de l'utilisateur du service vRealize Automation, un compte de domaine avec privilèges d'administrateur sur les serveurs Windows IaaS
- Noms de domaine complets des équilibres de charge
- Paramètres de la base de données SQL Server
- Paramètres d'agent proxy pour la connexion aux ressources de virtualisation
- Indique si le programme d'installation silencieuse doit tenter de corriger les conditions préalables manquantes du serveur Windows IaaS

Le programme d'installation silencieuse peut corriger de nombreuses conditions préalables Windows manquantes. Cependant, il ne peut pas corriger certains problèmes de configuration (comme un nombre insuffisant de CPU).

Pour gagner du temps, vous pouvez réutiliser et modifier un fichier `ha.properties` configuré pour un autre déploiement dont les paramètres étaient semblables. En outre, lorsque vous installez vRealize Automation de façon non silencieuse par le biais de l'assistant d'installation, l'assistant crée vos paramètres et les enregistre dans le fichier `ha.properties`. Ce fichier peut être utile pour effectuer des modifications en vue d'une réutilisation lors de l'installation silencieuse d'un déploiement semblable.

L'assistant n'enregistre pas les paramètres exclusifs, tels que les mots de passe, licences ou certificats, dans le fichier `ha.properties`.

La ligne de commande d'installation de vRealize Automation

vRealize Automation inclut une interface de ligne de commande basée sur une console pour l'exécution de réglages d'installation pouvant être requis après l'installation initiale.

L'interface de ligne de commande (CLI) peut exécuter des tâches d'installation et de configuration qui ne sont plus disponibles par le biais de l'interface basée sur le navigateur après l'installation initiale. Les fonctionnalités CLI incluent la vérification des conditions préalables, l'installation de composants IaaS, l'installation de certificats ou la définition du nom d'hôte vRealize Automation vers lequel les utilisateurs pointent leur navigateur Web.

L'interface de ligne de commande est également utile aux utilisateurs avancés qui souhaitent exécuter certaines opérations au moyen d'un script. Certaines fonctions de l'interface de ligne de commande sont utilisées par l'installation silencieuse, il convient donc de vous familiariser avec les deux fonctions pour renforcer vos connaissances sur l'écriture d'un script d'installation de vRealize Automation.

vRealize Automation Notions de base sur l'installation depuis la ligne de commande

L'interface de ligne de commande d'installation de vRealize Automation inclut des opérations de base de niveau supérieur.

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

`vra-command`

Afficher les ID de nœud

Il vous faut les ID de nœud vRealize Automation pour exécuter des commandes sur les systèmes cibles appropriés. Pour afficher les ID de nœud, entrez la commande suivante.

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

Notez les ID des nœuds avant d'exécuter des commandes sur des machines spécifiques.

Exécuter des commandes

La plupart des fonctions de ligne de commande impliquent l'exécution d'une commande sur un nœud dans le cluster vRealize Automation. Pour exécuter une commande, utilisez la syntaxe suivante.

```
vra-command execute --node node-ID command-name --parameter-name parameter-value
```

Comme le montre la syntaxe précédente, de nombreuses commandes nécessitent des paramètres et des valeurs de paramètres sélectionnés par l'utilisateur.

Afficher l'état d'une commande

Certaines commandes s'exécutent en quelques instants, d'autres sont plus longues. Pour surveiller l'avancement d'une commande qui a été soumise, entrez la commande suivante.

```
vra-command status
```

L'état de la commande est particulièrement pratique pour surveiller une installation silencieuse qui peut se prolonger pour les déploiements de grande taille.

Afficher l'aide

Pour afficher l'aide sur toutes les commandes disponibles, entrez la commande suivante.

```
vra-command help
```

Pour afficher de l'aide sur une commande spécifique, entrez la commande suivante.

```
vra-command help command-name
```

Noms des commandes d'installation de vRealize Automation

Les commandes vous donnent un accès par la console à de nombreuses tâches d'installation et de configuration de vRealize Automation que vous pouvez exécuter après l'installation initiale.

Les commandes disponibles mettent notamment en œuvre les fonctions suivantes.

- Ajout d'un autre dispositif vRealize Automation à une installation existante
- Définition du nom de l'hôte vers lequel les utilisateurs dirigent le navigateur Web lorsqu'ils accèdent à vRealize Automation
- Création de la base de données IaaS SQL Server
- Exécution de l'outil de vérification des conditions préalables sur un serveur IaaS Windows
- Importation de certificats

Pour la liste complète des commandes vRealize Automation disponibles, connectez-vous à la console du dispositif vRealize Automation, puis entrez la commande suivante.

```
vra-command help
```

La longue liste de noms de commandes et de paramètres n'est pas reproduite dans une documentation distincte. Pour utiliser la liste efficacement, identifiez une commande qui vous intéresse, puis ciblez de façon plus précise la demande en entrant la commande suivante.

```
vra-command help command-name
```

API d'installation de vRealize Automation

L'API REST de vRealize Automation pour l'installation vous donne la possibilité de créer des installations purement contrôlées par logiciel pour vRealize Automation.

L'API d'installation nécessite une version au format JSON des mêmes entrées qu'obtient l'installation depuis l'interface de ligne de commande à partir du fichier de réponse `ha.properties`. Les directives suivantes vous permettent de vous familiariser avec le fonctionnement de l'API. Vous pourrez ensuite concevoir des appels programmatiques de conception à l'API pour installer vRealize Automation.

- Pour accéder à la documentation de l'API, accédez à la page Web du dispositif vRealize Automation suivante.

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

Vous avez besoin d'un dispositif vRealize Automation non configuré. Reportez-vous à [Déployer le dispositif vRealize Automation](#).

- Pour expérimenter l'installation basée sur API, localisez et développez la commande PUT suivante.

```
PUT /vra-install
```

- Copiez le format JSON non renseigné de la zone **install_json** vers un éditeur de texte. Renseignez les valeurs de réponse de la même manière que vous le feriez pour `ha.properties`. Lorsque vos réponses au format JSON sont prêtes, recopiez le code dans **install_json** et remplacez le format JSON non renseigné.

Vous pouvez également modifier le modèle JSON suivant et copier les résultats dans **install_json**.

```
/usr/lib/vcac/tools/install/installationProperties.json
```

Vous pouvez également convertir un `ha.properties` renseigné en JSON ou vice versa.

- Dans la zone d'action, sélectionnez **validate** et cliquez sur **Try It Out**.

L'action de validation exécute l'utilitaire de vérification et de correction des conditions requises de vRealize Automation.

- La réponse de validation inclut un ID de commande alphanumérique que vous pouvez insérer dans la commande GET suivante.

```
GET /commands/command-id/aggregated-status
```

La réponse au GET inclut l'avancement de l'opération de validation.

- Lorsque la validation aboutit, vous pouvez exécuter l'installation proprement dite en recommençant le processus. Dans la zone d'action, sélectionnez simplement **install** plutôt que **validate**.

L'installation peut prendre un certain temps selon la taille du déploiement. De nouveau, localisez l'ID de commande, puis utilisez la commande GET d'état agrégé pour obtenir l'avancement de l'installation. La réponse GET peut ressembler à l'exemple suivant.

```
"progress": "78%", "counts": {"failed": 0, "completed": 14, "total": 18,
"queued": 3, "processing": 1}, "failed-commands": 0
```

- Si l'installation ne se déroule pas correctement, vous pouvez déclencher une collecte de journaux pour tous les nœuds à l'aide de la commande suivante.

```
PUT /commands/log-bundle
```

À l'instar de l'installation, l'ID de commande alphanumérique renvoyé vous permet de surveiller l'état de collecte de journaux.

Convertir entre propriétés silencieuses vRealize Automation et JSON

Pour les installations silencieuses de vRealize Automation avec l'interface de ligne de commande ou pour les installations basées sur API, vous pouvez convertir un fichier de réponse de propriétés renseigné en JSON ou vice versa. L'installation silencieuse sur interface de ligne de commande nécessite le fichier de propriétés, tandis que l'API nécessite un format JSON.

Conditions préalables

Un fichier de réponse de propriétés renseigné ou un fichier JSON renseigné

```
/usr/lib/vcac/tools/install/ha.properties.
```

ou

```
/usr/lib/vcac/tools/install/installationProperties.json
```

Procédure

- 1 Connectez-vous à une session de console de dispositif vRealize Automation en tant qu'utilisateur racine.
- 2 Exécutez le script de convertisseur approprié.
 - Convertissez JSON en propriétés

```
/usr/lib/vcac/tools/install/convert-properties --from-json
installationProperties.json
```

Le script crée un nouveau fichier de propriétés avec un nom incluant l'horodatage, par exemple :

```
ha.2016-10-17_13.02.15.properties
```


- Convertir des propriétés en JSON

```
/usr/lib/vcac/tools/install/convert-properties --to-json ha.properties
```

Le script crée un nouveau fichier `installationProperties.json` avec un nom incluant l'horodatage, par exemple :

```
installationProperties.2016-10-17_13.36.13.json
```

Résultats

Vous pouvez également afficher de l'aide pour le script.

```
/usr/lib/vcac/tools/install/convert-properties --help
```

Tâches post-installation vRealize Automation

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

Ne pas modifier le fuseau horaire vRealize Automation

Même si l'interface de gestion du dispositif vRealize Automation fournit une option pour la modifier, laissez toujours le fuseau horaire vRealize Automation défini sur Etc/UTC.

L'utilisation d'un fuseau horaire autre qu'Etc/UTC peut provoquer des erreurs inhabituelles telles que l'échec de migrations et des bundles de journaux qui ne contiennent pas les entrées provenant de tous les nœuds vRealize Automation.

L'option de l'interface de gestion du dispositif vRealize Automation que vous devez éviter se trouve sous **Système > Fuseau horaire**.

Configurer le chiffrement conforme à la norme de traitement des informations fédérales

Vous pouvez activer ou désactiver le chiffrement conforme à la norme FIPS (Federal Information Processing Standard) 140-2 pour le trafic réseau entrant et sortant du dispositif vRealize Automation.

La modification du paramètre FIPS nécessite un redémarrage de vRealize Automation. FIPS est désactivé par défaut.

Procédure

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

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

- 2 Cliquez sur **vRA > Paramètres de l'hôte**.

- 3 À proximité de l'angle droit supérieur, cliquez sur le bouton permettant d'activer ou de désactiver FIPS.

Lorsqu'il est activé, le trafic réseau entrant et sortant du dispositif vRealize Automation sur le port 443 utilise le chiffrement conforme à FIPS 140–2. Quel que soit le paramètre FIPS, vRealize Automation utilise des algorithmes conformes à AES–256 pour protéger les données sécurisées stockées sur le dispositif vRealize Automation.

Note Cette version de vRealize Automation assure uniquement partiellement la conformité FIPS, car certains composants internes n'utilisent pas encore des modules de chiffrement certifiés. Lorsque les modules certifiés n'ont pas encore été mis en œuvre, les algorithmes conformes à AES–256 sont utilisés.

- 4 Cliquez sur **Oui** pour redémarrer vRealize Automation.

Résultats

Vous pouvez également configurer FIPS à partir d'une session de console de dispositif vRealize Automation en tant qu'utilisateur racine en utilisant les commandes suivantes.

```
vcac-vami fips enable
vcac-vami fips disable
vcac-vami fips status
```

Activer le basculement automatique de Manager Service

Le basculement automatique de Manager Service est désactivé par défaut si vous installez ou mettez à niveau Manager Service avec le programme d'installation de Windows vRealize Automation standard.

Pour activer le basculement automatique de Manager Service après avoir exécuté le programme d'installation standard de Windows, procédez comme suit.

Dans une configuration à plusieurs nœuds, vous n'avez besoin d'effectuer les étapes qu'une seule fois, sur n'importe quel nœud de dispositif vRealize Automation.

Procédure

- 1 Connectez-vous en tant qu'utilisateur racine à une session de console sur le dispositif vRealize Automation.
- 2 Accédez au répertoire suivant :
`/usr/lib/vcac/tools/vami/commands`
- 3 Entrez la commande suivante :
`python ./manager-service-automatic-failover ENABLE`

Résultats

Si vous devez désactiver le basculement automatique dans un déploiement IaaS, entrez la commande suivante à la place.

```
python ./manager-service-automatic-failover DISABLE
```

À propos du basculement automatique de Manager Service

Vous pouvez configurer vRealize Automation IaaS Manager Service pour basculer automatiquement sur une sauvegarde si l'instance principale de Manager Service s'arrête.

À partir de vRealize Automation 7.3, vous n'avez plus besoin de démarrer ou d'arrêter Manager Service manuellement sur chaque serveur Windows pour contrôler lequel est utilisé comme serveur principal ou de secours. Le basculement automatique de Manager Service est activé par défaut dans les cas suivants.

- Lorsque vous installez vRealize Automation en mode silencieux ou avec l'assistant d'installation
- Lorsque vous mettez à niveau IaaS via l'interface d'administration ou avec le script de mise à niveau automatique.

Le basculement n'est pas activé lorsque le programme d'installation basé sur Windows standard permet d'ajouter un hôte Manager Service ou de mettre à niveau IaaS. Pour l'activer, consultez [Activer le basculement automatique de Manager Service](#).

Lorsque le basculement automatique est activé, Manager Service démarre automatiquement sur tous les hôtes Manager Service, y compris les sauvegardes. La fonctionnalité de basculement automatique permet aux hôtes de se surveiller mutuellement de manière transparente et de basculer si nécessaire. La fonctionnalité requiert que le service Windows soit en cours d'exécution sur tous les hôtes.

Note Vous n'êtes pas obligé d'utiliser le basculement automatique. Vous pouvez le désactiver et continuer de démarrer et d'arrêter manuellement le service Windows pour contrôler quel hôte sert d'hôte principal ou de sauvegarde. Si vous choisissez le basculement manuel, il vous suffit de démarrer le service sur un hôte à la fois. Avec le basculement automatique désactivé, l'exécution simultanée du service sur plusieurs serveurs IaaS rend vRealize Automation inutilisable.

Ne tentez pas d'activer ou de désactiver de manière sélective le basculement automatique. Le basculement automatique doit toujours être synchronisé, qu'il soit sous tension ou hors tension, sur chaque hôte Manager Service dans un déploiement IaaS.

Si le basculement automatique ne semble pas fonctionner, reportez-vous à la section [Impossible d'activer le basculement automatique de Manager Service](#) pour obtenir des conseils sur le dépannage.

Pour plus d'informations sur la façon d'équilibrer la charge de travail d'hôtes Manager Service, reportez-vous à [Équilibrage de charge de vRealize Automation](#).

Basculement de la base de données PostgreSQL vRealize Automation automatique

Dans un déploiement vRealize Automation à haute disponibilité, certaines configurations autorisent la base de données PostgreSQL vRealize Automation intégrée à basculer automatiquement.

Le basculement automatique est activé en mode silencieux dans les conditions suivantes.

- Le déploiement haute disponibilité inclut trois dispositifs vRealize Automation.
Le basculement automatique n'est pas pris en charge avec seulement deux dispositifs.
- La réplication de la base de données est définie sur le mode synchrone sous l'onglet Cluster de l'interface d'administration de vRealize Automation.

En règle générale, évitez d'effectuer un basculement manuel alors que le basculement automatique est activé. Toutefois, en cas de problèmes de nœud, le basculement automatique peut ne pas se produire même s'il est activé. Le cas échéant, vérifiez si vous avez besoin d'effectuer un basculement manuel.

- 1 Une fois que le nœud de base de données PostgreSQL principal échoue, attendez jusqu'à 5 minutes pour que le reste du cluster se stabilise.
- 2 Sur un nœud de dispositif vRealize Automation encore fonctionnel, ouvrez un navigateur avec l'URL suivante.

`https://vrealize-automation-appliance-FQDN:5434/api/status`

- 3 Recherchez `manualFailoverNeeded`.
- 4 Si `manualFailoverNeeded` est vraie, effectuez un basculement manuel.

Pour plus d'informations, reportez-vous au manuel [Effectuer le basculement de base de données du dispositif vRealize Automation](#).

Remplacement de certificats autosignés par des certificats fournis par une autorité

Si vous avez installé vRealize Automation avec des certificats autosignés, vous pouvez décider de les remplacer par des certificats fournis par une autorité de certification avant d'effectuer un déploiement dans un environnement de production.

Pour plus d'informations sur la mise à jour des certificats, reportez-vous à la section [Mise à jour des certificats vRealize Automation](#).

Modification de noms d'hôtes et d'adresses IP

En règle générale, il est recommandé de conserver les noms d'hôtes, les noms de domaine complets et les adresses IP que vous avez prévu d'utiliser pour les systèmes vRealize Automation. Certaines modifications post-installation sont possibles, mais peuvent s'avérer complexes.

- Si vous modifiez le nom d'hôte de la machine Windows qui héberge la base de données SQL Server IaaS, reportez-vous à la section [Configurer la base de données SQL pour un nouveau nom d'hôte](#).

- Lors de la restauration des composants IaaS, le fait de renommer un hôte peut affecter l'hôte IaaS Web, l'hôte Manager Service ou leurs équilibres de charge respectifs. Restaurez ces hôtes ou ces équilibres de charge en fonction de la sauvegarde de *vRealize Suite* et des instructions de restauration.

Pour modifier le nom d'hôte ou l'adresse IP d'un dispositif vRealize Automation, reportez-vous aux sections suivantes.

Modifier le nom d'hôte du dispositif vRealize Automation

Lors de la maintenance d'un environnement ou d'un réseau, vous devrez éventuellement attribuer un nom d'hôte différent à un dispositif vRealize Automation.

Important Le changement de nom met vRealize Automation hors ligne pendant plusieurs minutes.

Les mêmes étapes s'appliquent aux dispositifs vRealize Automation autonomes, maîtres et répliques.

Procédure

- 1 Dans DNS, créez un enregistrement supplémentaire avec le nouveau nom d'hôte du nœud.
Ne supprimez pas l'enregistrement DNS portant l'ancien nom d'hôte pour l'instant.
- 2 Attendez la réplication DNS et la distribution de zone.
- 3 Connectez-vous à la ligne de commande du dispositif vRealize Automation en tant qu'utilisateur racine.
- 4 Exécutez la commande suivante.

```
vcac-config hostname-change --host new-hostname --certificate certificate-file-name
```

Un fichier de certificat est facultatif, sauf si l'ancien nom d'hôte de dispositif a été utilisé dans un certificat. Si c'est le cas, fournissez un certificat mis à jour comprenant le nouveau nom d'hôte.

Lorsque vous spécifiez un fichier de certificat, la commande de changement de nom importe également le certificat et renvoie son ID.

Un fichier de certificat doit être au même format que la sortie de texte de la commande d'API `/config/ssl/generate-certificate` et contenir le nouveau nom DNS dans son champ SAN.

- 5 Patientez 15 minutes ou plus jusqu'à la fin du processus de changement de nom. Les actions de commande prennent quelques minutes, suivies de plusieurs minutes supplémentaires de réinscription du service.
- 6 Si l'ancien nom d'hôte de dispositif a été utilisé avec un équilibre de charge dans un environnement HA, vérifiez et reconfigurez l'équilibre de charge avec le nouveau nom.
- 7 Dans DNS, supprimez l'ancien enregistrement DNS portant l'ancien nom d'hôte.

Résultats

Si vous avez des difficultés pour changer un nom d'hôte, essayez plutôt les procédures distinctes de la documentation de vRealize Automation 7.3.

Modifier l'adresse IP du dispositif vRealize Automation

Lors de la maintenance d'un environnement ou d'un réseau, vous devrez éventuellement attribuer une adresse IP différente à un dispositif vRealize Automation existant.

Conditions préalables

- Par précaution, prenez des snapshots des dispositifs vRealize Automation et des serveurs IaaS.
- À partir d'une session de console en tant qu'utilisateur racine sur les dispositifs vRealize Automation, inspectez les entrées du fichier `/etc/hosts`.

Recherchez les attributions d'adresses pouvant entrer en conflit avec le nouveau plan d'adressage IP et apportez les modifications nécessaires.

Sur tous les serveurs IaaS, répétez la procédure pour le fichier `Windows\system32\drivers\etc\hosts`.

- Arrêtez tous les dispositifs vRealize Automation.
- Arrêtez tous les services vRealize Automation sur les serveurs IaaS.

Procédure

- 1 Dans vSphere, localisez le dispositif vRealize Automation que vous souhaitez modifier et sélectionnez **Actions > Modifier les paramètres**.
- 2 Cliquez sur **Options vApp**.
- 3 Développez **Allocation d'adresses IP** et activez l'option **Environnement OVF**.

4 Développez **Paramètres OVF** et activez l'option **Image ISO**.

The screenshot shows the 'vApp Options' tab with the following settings:

- IP allocation** (expanded):
 - IP allocation scheme: A vApp can obtain its network configuration through the OVF environment or a DHCP server. Specify the network configuration schemes supported by this vApp:
 - ☐ DHCP
 - ☒ **OVF environment**
 - IP protocol: Specify the IP protocols supported by this vApp:
 - Both
- OVF settings** (expanded):
 - OVF environment: View...
 - OVF environment transport:
 - ☒ **ISO image**
 - ☒ VMware Tools
 - Installation boot:
 - ☐ Enable
 - 0

5 Cliquez sur **OK**.

6 Démarrez le dispositif vRealize Automation que vous modifiez.

7 Connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.

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

8 Cliquez sur l'onglet **Réseau**.

9 Sous les onglets, cliquez sur **Adresse**.

10 Mettez à jour l'adresse IP.

11 Dans le coin supérieur droit, cliquez sur **Enregistrer les paramètres**.

12 Arrêtez le dispositif vRealize Automation que vous modifiez.

13 Dans DNS, mettez à jour les entrées des nouvelles adresses IP.

Mettez uniquement à jour les enregistrements de type A existants. Ne modifiez pas les noms de domaine complets.

Si vous utilisez un équilibrage de charge, mettez également à jour les paramètres IP d'équilibrage de charge pour les nœuds principaux, les pools de service et les serveurs virtuels selon les besoins.

14 Attendez la réplication DNS et la distribution de zone.

- 15 Démarrez tous les dispositifs vRealize Automation.
- 16 Démarrez les services vRealize Automation sur les serveurs IaaS.
- 17 Connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.

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

- 18 Vérifiez l'état du dispositif vRealize Automation dans les zones suivantes.

- État de la connexion à la base de données sous **Cluster**
- État de RabbitMQ sous **vRA > Messagerie**
- État de Xenon sous **vRA > Xenon**
- Tous les services ENREGISTRÉ sous **Services**

Ajuster la base de données SQL pour un nom d'hôte modifié

Vous devez réviser les paramètres de configuration si vous déplacez la base de données SQL vRealize Automation IaaS vers un autre nom d'hôte.

Sur le même nom d'hôte, vous pouvez restaurer la base de données SQL à partir d'une sauvegarde, sans étapes supplémentaires requises. Si vous effectuez une restauration vers un nom d'hôte différent, vous devez modifier les fichiers de configuration afin d'apporter des modifications supplémentaires.

Consultez [Article 2074607 de la base de connaissances VMware](#) pour les modifications requises lors du déplacement de la base de données SQL vers un nom d'hôte différent.

Modifier l'adresse IP d'un serveur IaaS

Lors de la maintenance d'un environnement ou d'un réseau, vous devrez éventuellement attribuer une adresse IP différente à un serveur Windows vRealize Automation IaaS existant.

Conditions préalables

- Si l'adresse IP du dispositif vRealize Automation doit être modifiée, effectuez d'abord cette modification. Reportez-vous à [Modifier l'adresse IP du dispositif vRealize Automation](#).
- Par précaution, prenez des snapshots des dispositifs vRealize Automation et des serveurs IaaS.
- À partir d'une session de console en tant qu'utilisateur racine sur le dispositif vRealize Automation, inspectez les entrées du fichier `/etc/hosts`.

Recherchez les attributions d'adresses pouvant entrer en conflit avec le nouveau plan d'adressage IP et apportez les modifications nécessaires.

Sur tous les serveurs IaaS, répétez la procédure pour le fichier `Windows\system32\drivers\etc\hosts`.

- Arrêtez le dispositif vRealize Automation.

- Arrêtez tous les services vRealize Automation sur les serveurs IaaS.

Procédure

- 1 Connectez-vous au serveur IaaS en utilisant un compte ayant des droits d'administrateur.

- 2 Dans Windows, modifiez l'adresse IP.

Recherchez l'adresse IP dans la fenêtre Paramètres de l'adaptateur réseau Windows, sous les propriétés du protocole Internet.

- 3 Actualisez votre DNS local avec les modifications.

L'actualisation de DNS garantit que les serveurs Windows IaaS peuvent se trouver et que vous pouvez vous reconnecter à un serveur Windows si vous êtes déconnecté.

- 4 Sur l'hôte Manager Service, examinez le fichier suivant dans un éditeur de texte.

install-folder\VCAC\Server\ManagerService.exe.config

Le dossier d'installation par défaut est C:\Program Files (x86)\VMware.

Vérifiez les adresses IP ou les noms de domaine complets des dispositifs vRealize Automation et des serveurs Windows IaaS.

- 5 Sur tous les serveurs Windows IaaS, examinez le fichier suivant dans un éditeur de texte.

install-folder\VCAC\Management Agent\VMware.IaaS.Management.Agent.exe.Config

Vérifiez l'adresse IP ou le nom de domaine complet du dispositif vRealize Automation.

- 6 Connectez-vous à l'hôte SQL Server.

- 7 Vérifiez que l'adresse du référentiel est correctement configurée pour utiliser le nom de domaine complet dans la colonne ConnectionString.

Par exemple, ouvrez SQL Management Studio et exécutez la requête suivante.

```
"SELECT Name, ConnectionString FROM [database-name].[DynamicOps.RepositoryModel].[Models]"
```

- 8 Démarrez le dispositif vRealize Automation.

- 9 Démarrez les services vRealize Automation sur les serveurs IaaS.

- 10 Examinez les fichiers journaux pour vérifier que les services d'agent, de DEM Worker, de Manager Service et d'hôte Web ont bien démarré.

- 11 Connectez-vous à vRealize Automation en tant qu'utilisateur disposant du rôle d'administrateur d'infrastructure.

- 12 Accédez à **Infrastructure > Surveillance > État d'exécution distribuée** et vérifiez que tous les services sont en cours d'exécution.

- 13 Testez le bon fonctionnement en vérifiant les services de dispositif, en testant le provisionnement, ou en utilisant l'outil de test de production vRealize.

Modifier un nom d'hôte de serveur IaaS

Lors de la maintenance d'un environnement ou d'un réseau, vous devrez éventuellement attribuer un nom d'hôte différent à un serveur Windows vRealize Automation IaaS existant.

Procédure

- 1 Prenez un snapshot du serveur IaaS.
- 2 Sur le serveur IaaS, utilisez IIS Manager pour arrêter les pools d'applications vRealize Automation : Repository, VMware vRealize Automation et Wapi.
- 3 Sur le serveur IaaS, utilisez les Outils administrateur > Services pour arrêter tous les services, agents et DEM vRealize Automation.
- 4 Dans DNS, créez un enregistrement supplémentaire avec le nouveau nom d'hôte.
Ne supprimez pas l'enregistrement DNS portant l'ancien nom d'hôte pour l'instant.
- 5 Attendez la réplication DNS et la distribution de zone.
- 6 Sur le serveur IaaS, modifiez le nom d'hôte mais ne redémarrez pas lorsque vous y êtes invité.
Recherchez le nom d'hôte dans les propriétés du système Windows, sous le nom de l'ordinateur, le domaine et les paramètres du groupe de travail.
Lorsque vous êtes invité à redémarrer, cliquez sur l'option pour redémarrer plus tard.
- 7 Si vous avez utilisé l'ancien nom d'hôte pour générer des certificats, mettez à jour les certificats.
Pour plus d'informations, reportez-vous à la section [Mise à jour de certificats vRealize Automation](#).
- 8 Utilisez un éditeur de texte pour localiser et mettre à jour le nom d'hôte à l'intérieur des fichiers de configuration.
Effectuez les mises à jour en fonction du nom d'hôte du serveur IaaS que vous avez modifié.
Dans un déploiement distribué HA, vous devrez peut-être accéder à plusieurs serveurs. Il n'existe aucune mise à jour si vous modifiez le nom d'hôte d'un composant DEM Orchestrator ou DEM Worker.

Note Mettre à jour uniquement l'ancien nom d'hôte de serveur Windows. Si à la place, vous trouvez un nom d'équilibrage de charge, conservez-le.

Tableau 1-38. Fichiers à mettre à jour lorsque vous modifiez un nom d'hôte du nœud Web

Serveur IaaS	Chemin d'accès	Fichier
Nœuds Web	<i>install-folder</i> \Server\Website	Web.config
	<i>install-folder</i> \Server\Website\Cafe	Vcac-Config.exe.config
	<i>install-folder</i> \Web API	Web.config
	<i>install-folder</i> \Web API\ConfigTool	Vcac-Config.exe.config

Tableau 1-38. Fichiers à mettre à jour lorsque vous modifiez un nom d'hôte du nœud Web (suite)

Serveur IaaS	Chemin d'accès	Fichier
Nœud avec le composant Model Manager installé	<i>install-folder\Server\Model Manager Data</i>	Repoutil.exe.config
	<i>install-folder\Server\Model Manager Data\Cafe</i>	Vcac-Config.exe.config
Nœuds Manager Service	<i>install-folder\Server</i>	ManagerService.exe.config
Nœuds DEM Orchestrator	<i>install-folder\Distributed Execution Manager\dem</i>	DynamicOps.DEM.exe.config
Nœuds DEM Worker	<i>install-folder\Distributed Execution Manager\DEM-name</i>	DynamicOps.DEM.exe.config
Nœuds Agent	<i>install-folder\Agents\agent-name</i>	RepoUtil.exe.config
	<i>install-folder\Agents\agent-name</i>	VRMAgent.exe.config

Tableau 1-39. Fichiers à mettre à jour lorsque vous modifiez un nom d'hôte du nœud Manager Service

Serveur IaaS	Chemin d'accès	Fichier
Nœuds DEM Orchestrator	<i>install-folder\Distributed Execution Manager\DEM-name</i>	DynamicOps.DEM.exe.config
Nœuds DEM Worker	<i>install-folder\Distributed Execution Manager\dem</i>	DynamicOps.DEM.exe.config
Nœuds Agent	<i>install-folder\Agents\agent-name</i>	VRMAgent.exe.config

Tableau 1-40. Fichiers à mettre à jour lorsque vous modifiez un nom d'hôte du nœud Agent

Serveur IaaS	Chemin d'accès	Fichier
Nœud Agent	<i>install-folder\Agents\agent-name</i>	VRMAgent.exe.config

- 9 Redémarrez le serveur IaaS pour lequel vous avez modifié le nom d'hôte.
- 10 Démarrez les pools d'applications vRealize Automation que vous avez arrêtés précédemment.
- 11 Démarrez les services, les agents et les composants DEM vRealize Automation que vous avez arrêtés précédemment.
- 12 Si l'ancien nom d'hôte du serveur IaaS était utilisé avec un équilibrage de charge dans un environnement HA, vérifiez et reconfigurez l'équilibrage de charge avec le nouveau nom.
- 13 Dans DNS, supprimez l'ancien enregistrement DNS portant l'ancien nom d'hôte.
- 14 Attendez la réplication DNS et la distribution de zone.

15 Si vous avez modifié le nom d'un hôte Manager Service, exécutez les étapes supplémentaires suivantes.

- a Mettez à jour les agents logiciels sur les machines virtuelles existantes.
- b Recréez les images ISO ou les modèles qui contiennent un agent invité.

Étape suivante

Confirmer que vRealize Automation est prêt à être utilisé. Consultez la documentation de [Sauvegarde et restauration de vRealize Suite](#).

Définissez l'URL de connexion à vRealize Automation sur un nom personnalisé

Si vous souhaitez que les utilisateurs de vRealize Automation se connectent à un nom d'URL autre que le nom du dispositif vRealize Automation ou le nom de l'équilibrage de charge, suivez les étapes de personnalisation avant et après l'installation.

Procédure

- 1** Avant de procéder à l'installation, préparez un certificat qui inclut le CNAME que vous le souhaitez utiliser, ainsi que les noms du dispositif vRealize Automation et de l'équilibrage de charge.
- 2** Installez vRealize Automation, en entrant le nom du dispositif ou de l'équilibrage de charge comme d'habitude. Pendant l'installation, importez le certificat personnalisé.
- 3** Après l'installation, dans DNS, créez un alias CNAME Nom commun et pointez-le vers l'adresse VIP du dispositif ou de l'équilibrage de charge.
- 4** Connectez-vous à l'interface de l'administrateur de dispositif vRealize Automation en tant qu'utilisateur racine.

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

- 5** Sous **vRA > Paramètres de l'hôte**, remplacez le **Nom d'hôte** par le CNAME que vous avez choisi.

Supprimer un nœud du dispositif vRealize Automation

Lors de la maintenance d'un environnement HA, vous devrez peut-être supprimer un nœud du dispositif vRealize Automation défaillant à partir du cluster.

Pour supprimer un nœud, suivez les instructions de [Pour supprimer un dispositif, suivez les instructions de l'article 2149866 de la Base de connaissances VMware](#).

Installation de l'agent vRealize Log Insight sur des serveurs IaaS

Les serveurs Windows dans une configuration vRealize Automation IaaS n'incluent pas l'agent vRealize Log Insight par défaut.

vRealize Log Insight fournit une agrégation et une indexation de journaux, et peut collecter, importer et analyser des journaux pour exposer des problèmes du système. Si vous souhaitez capturer et analyser des journaux des serveurs IaaS en utilisant vRealize Log Insight, vous devez installer séparément l'agent vRealize Log Insight pour Windows.

Pour plus d'informations, reportez-vous à la [documentation de VMware vRealize Log Insight](#).

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

Modifier le port de proxy de VMware Remote Console

Si votre site bloque ou réserve le port 8444, vous pouvez modifier le port de proxy par défaut utilisé par VMware Remote Console.

Procédure

- 1 Accédez à l'invite de commande du dispositif vRealize Automation en tant qu'utilisateur racine.
- 2 Ouvrez le fichier suivant dans un éditeur de texte.
`/etc/vcac/security.properties`
- 3 Remplacez la valeur par défaut 8444 de `consoleproxy.service.port` par un port inutilisé.
- 4 Enregistrez et fermez `security.properties`.
- 5 Redémarrez le dispositif vRealize Automation.

Résultats

Dans un environnement HA, apportez la même modification à tous les dispositifs vRealize Automation.

Modifier un nom de domaine complet du dispositif vRealize Automation et lui attribuer le nom de domaine complet d'origine

Dans certains cas, un nom de domaine complet du dispositif vRealize Automation peut changer lorsque vous ne le souhaitez pas. Par exemple, le nom de domaine complet change si vous créez un répertoire Integrated Windows Authentication (IWA) pour un domaine autre que le domaine sur lequel se trouve le dispositif.

Si vous créez un répertoire IWA pour un autre domaine, suivez les étapes suivantes pour modifier le nom de domaine complet du dispositif et lui attribuer le nom de domaine complet d'origine.

Procédure

- 1 Connectez-vous à vRealize Automation et créez l'annuaire IWA comme vous le feriez normalement.
Consultez [Configurer un lien Active Directory utilisant le protocole LDAP/IWA](#)
- 2 S'il s'agit d'un environnement HA, suivez également les étapes du document [Configuration de la gestion des annuaires pour haute disponibilité](#).

- 3 La création d'un répertoire IWA pour un domaine autre que celui sur lequel se trouve un dispositif modifie discrètement le nom de domaine complet du dispositif.

Par exemple, va1.domain1.local devient va1.domain2.local lorsque vous créez un répertoire IWA pour domain2.local.

Annuler la modification en renommant chaque dispositif avec son nom de domaine complet d'origine. Reportez-vous à la procédure associée dans [Modification de noms d'hôtes et d'adresses IP](#).

- 4 Une fois que les dispositifs sont complètement en ligne avec leur nom de domaine complet d'origine, connectez-vous à chaque nœud IaaS et suivez les étapes suivantes.

- a Ouvrez le fichier suivant dans un éditeur de texte.

```
C:\Program Files (x86)\VMware\VCAC\Management Agent
\VMware.IaaS.Management.Agent.exe.Config
```

- b Modifier chaque nom de domaine complet de endpoint address= du dispositif et leur attribuer le nom de domaine complet d'origine.

Par exemple, à partir de :

```
<endpoint address="https://va1.domain2.local:5480/"
thumbprint="90C55BAEC53E31609EE1614CE4A8336848A8D4CF" />
<endpoint address="https://va2.domain2.local:5480/"
thumbprint="0468BF6EDBC6F2209BE01D0D7FD1094197E324ED" />
```

Au :

```
<endpoint address="https://va1.domain1.local:5480/"
thumbprint="90C55BAEC53E31609EE1614CE4A8336848A8D4CF" />
<endpoint address="https://va2.domain1.local:5480/"
thumbprint="0468BF6EDBC6F2209BE01D0D7FD1094197E324ED" />
```

- c Enregistrez et fermez VMware.IaaS.Management.Agent.exe.Config.

- 5 Connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.

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

- 6 Accédez à **vRA > Messagerie** et cliquez sur **Réinitialiser le cluster RabbitMQ**.

- 7 Une fois la réinitialisation terminée, connectez-vous à chaque interface de gestion de dispositif.

- 8 Accédez à **Cluster**, puis vérifiez que tous les nœuds sont connectés au cluster.

Configurer le groupe de disponibilité AlwaysOn SQL

Vous devez apporter des modifications de configuration si vous définissez le groupe de disponibilité AlwaysOn (AAG) SQL après l'installation de vRealize Automation.

Lorsque vous configurez le groupe AAG SQL après l'installation, suivez les étapes de [Article 2074607 de la base de connaissances VMware](#) pour configurer vRealize Automation avec le nom de domaine complet de l'écouteur AAG en tant qu'hôte SQL Server.

Ajouter des contrôleurs d'interface réseau après l'installation de vRealize Automation

vRealize Automation prend en charge plusieurs contrôleurs d'interface réseau (NIC). Après l'installation, vous pouvez ajouter des cartes réseau au dispositif vRealize Automation ou au serveur Windows IaaS.

Plusieurs cartes réseau peuvent être nécessaires pour certains déploiements vRealize Automation, par exemple :

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

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

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

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

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

Conditions préalables

Installez complètement vRealize Automation dans votre environnement vCenter.

Procédure

- 1 Dans vCenter, ajoutez des cartes réseau à chaque dispositif vRealize Automation.
 - a Cliquez avec le bouton droit sur le dispositif et sélectionnez **Modifier les paramètres**.
 - b Ajoutez des cartes réseau VMXNETn.
 - c S'il est sous tension, redémarrez le dispositif.

- 2 Connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.

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

- 3 Sélectionnez **Réseau**, puis vérifiez que plusieurs cartes réseau sont disponibles.
- 4 Sélectionnez **Adresse** et configurez l'adresse IP des cartes réseau.

Tableau 1-41. Exemple de configuration de carte réseau

Configuration	Valeur
Type d'adresse IPv4	Statique
Adresse IPv4	172.22.0.2
Masque de réseau	255.255.255.0

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

Étape suivante

(Facultatif) Si vous avez besoin d'itinéraires statiques, consultez [Configurer des routes statiques](#).

Configurer des routes statiques

Lors de l'ajout de cartes réseau à une installation vRealize Automation, si vous avez besoin de routes statiques, vous ouvrez une session d'invite de commandes pour les configurer.

Conditions préalables

Ajoutez plusieurs cartes réseau à des dispositifs vRealize Automation ou à des serveurs Windows IaaS.

Procédure

- 1 Connectez-vous à la ligne de commande du dispositif vRealize Automation en tant qu'utilisateur racine.

- 2 Ouvrez le fichier d'itinéraires dans un éditeur de texte.

```
/etc/sysconfig/network/routes
```

- 3 Recherchez la ligne `default` pour la passerelle par défaut, mais ne la modifiez pas.

Note Dans les cas où il faut changer la passerelle par défaut, utilisez plutôt l'interface de gestion de vRealize Automation.

- 4 Sous la ligne `default`, ajoutez de nouvelles lignes pour les itinéraires statiques. Par exemple :

```
default 10.10.10.1 - -
172.30.30.0 192.168.100.1 255.255.255.0 eth0
192.168.210.0 192.168.230.1 255.255.255.0 eth2
```

- 5 Enregistrez et fermez le fichier d'itinéraires.
- 6 Redémarrez le dispositif .
- 7 Dans les clusters HA, répétez le processus pour chaque dispositif.
- 8 Connectez-vous au serveur Windows IaaS en tant qu'administrateur.
- 9 Ouvrez une invite de commandes en tant qu'administrateur.
- 10 Pour configurer un itinéraire statique, entrez la commande `route -p add`, où `-p` maintient l'itinéraire statique lors des redémarrages successifs. Par exemple :

```
C:\Windows\system32> route -p add 172.30.30.0 mask 255.255.255.0 192.168.100.1 metric 1
OK!
```

Pour plus d'informations sur la configuration des itinéraires statiques dans Windows, consultez la documentation de Microsoft.

Gestion des correctifs accés

Le support technique pour votre installation vRealize Automation peut impliquer un correctif logiciel que vous installez ou supprimez à l'aide de l'interface de gestion de dispositif vRealize Automation.

Pour vous aider à résoudre les problèmes qui peuvent se produire pratiquement en temps réel, des instructions relatives aux correctifs, aux conditions préalables et à l'installation sont disponibles dans la [Base de connaissances VMware](#). Par exemple, l'[article 60310 de la base de connaissances VMware](#) est surveillé et mis à jour avec les dernières informations de correctif vRealize Automation 7.5.

L'interface de correctif ne peut pas appliquer de correctif aux composants vRealize Automation suivants.

- L'agent de gestion
- Agents non vSphere, tel que XenServer, VDI ou Hyper-V

Procédure

- 1 Connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Cliquez sur **vRA > Correctifs**.
- 3 Sous Gestion des correctifs, cliquez sur l'option dont vous avez besoin et suivez les invites.

Option	Description
Nouveau correctif	Installez un nouveau correctif que vous avez téléchargé.
Correctifs installés	Ajoutez le correctif récemment installé aux nœuds de cluster récemment ajoutés.
Retour arrière	Supprimez le correctif le plus récemment installé et restaurez vRealize Automation au niveau de correctif précédent.
Historique	Examinez la liste des correctifs installés et supprimés.

Pour activer ou désactiver la gestion des correctifs, connectez-vous à l'invite de commandes du dispositif vRealize Automation en tant qu'utilisateur racine et entrez l'une des commandes suivantes.

```
/opt/vmware/share/htdocs/service/hotfix/scripts/hotfix.sh enable
/opt/vmware/share/htdocs/service/hotfix/scripts/hotfix.sh disable
```

Configurer l'accès au locataire par défaut

Vous devez octroyer à votre équipe des droits d'accès au locataire par défaut avant qu'elle puisse configurer vRealize Automation.

Le locataire par défaut est automatiquement créé lorsque vous configurez l'assistant d'installation de single sign-on. Vous ne pouvez pas modifier les détails du locataire, par exemple le nom ou le jeton URL, mais vous pouvez créer de nouveaux utilisateurs locaux et nommer des administrateurs de locataire ou IaaS supplémentaires à tout moment.

Procédure

- 1 Connectez-vous à vRealize Automation en tant qu'administrateur du locataire par défaut.
 - a Accédez à l'interface du produit vRealize Automation.
`https://vrealize-automation-FQDN/vcac`
 - b Connectez-vous avec le nom d'utilisateur **administrateur** et le mot de passe que vous avez défini pour cet utilisateur lorsque vous avez configuré SSO.
- 2 Sélectionnez **Administration > Locataires**.
- 3 Cliquez sur le nom du locataire par défaut, **vsphere.local**.
- 4 Cliquez sur l'onglet **Utilisateurs locaux**.

5 Créez des comptes d'utilisateurs locaux pour le locataire vRealize Automation par défaut.

Les utilisateurs locaux sont spécifiques au locataire et peuvent uniquement accéder au locataire dans lequel vous les avez créés.

- a Cliquez sur l'icône Ajouter (+).
- b Entrez les détails de l'utilisateur responsable de l'administration de votre infrastructure.
- c Cliquez sur **Ajouter**.
- d Recommencez ces étapes pour ajouter un ou plusieurs utilisateurs supplémentaires responsables de la configuration du locataire par défaut.

6 Cliquez sur l'onglet **Administrateurs**.

7 Attribuez à vos utilisateurs locaux les rôles d'administrateur de locataires et d'administrateur 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**.

Étape suivante

Fournissez à votre équipe l'URL d'accès et les informations de connexion aux comptes d'utilisateurs que vous avez créés afin qu'ils puissent commencer la configuration de vRealize Automation.

- Vos administrateurs de locataire configurent des paramètres comme l'authentification d'utilisateur, notamment la configuration de Gestion des annuaires pour la haute disponibilité. Reportez-vous à la section [Configuration des paramètres de locataire](#).
- Vos administrateurs IaaS préparent des ressources externes à des fins de provisionnement. Reportez-vous à la section [Préparations externes pour le provisionnement](#)
- Si vous avez configuré la création de contenu initial pendant l'installation, votre administrateur de configuration peut demander à l'élément du catalogue Contenu initial de renseigner rapidement une validation technique.

Dépannage de l'installation de vRealize Automation

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.

Emplacement des journaux par défaut

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

Note Pour la collecte de journaux, vous pouvez tirer parti des packs de contenu vRealize Automation et vRealize Orchestrator pour vRealize Log Insight. Les packs de contenu et Log Insight fournissent un résumé consolidé des événements du journal pour les composants de vRealize Suite. Pour en savoir plus, consultez le site [VMware Solution Exchange](#).

Pour consulter la liste des emplacements des journaux la plus récente, reportez-vous à [Article 2141175 de la base de connaissances VMware](#).

Journaux Windows

Utilisez l'emplacement suivant pour trouver les fichiers journaux d'événements Windows.

Journal	Emplacement
Journaux de l'Observateur d'événements Windows	Démarrer > Panneau de configuration > Outil d'administration > Observateur d'événements

Journaux d'installation

Les journaux d'installation se trouvent aux emplacements suivants.

Journal	Emplacement par défaut
Journaux d'installation	C:\Program Files (x86)\vCAC\InstallLogs C:\Program Files (x86)\VMware\vCAC\Server\ConfigTool\Log
Journaux d'installation WAPI	C:\Program Files (x86)\VMware\vCAC\Web API\ConfigTool\Logfilename WapiConfiguration-<XXX>

Journaux IaaS

Les journaux IaaS se trouvent aux emplacements suivants.

Journal	Emplacement par défaut
Journaux de site Web	C:\Program Files (x86)\VMware\vCAC\Server\Website\Logs
Journal de référentiel	C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Web\Logs
Journaux de Manager Service	C:\Program Files (x86)\VMware\vCAC\Server\Logs
Journaux de DEM Orchestrator	C:\Users\<user-name>\AppData\Local\Temp\VMware\vCAC\Distributed Execution Manager\<system-name> DEO \Logs
Journaux d'agents	C:\Users\<user-name>\AppData\Local\Temp\VMware\vCAC\Agents\<agent-name>\logs

Journaux de l'infrastructure vRealize Automation

Les entrées de journaux pour les infrastructures vRealize Automation se trouvent à l'emplacement suivant.

Journal	Emplacement par défaut
Journaux de l'infrastructure	/var/log/vmware

Journaux de provisionnement des composants logiciels

Les journaux de provisionnement des composants logiciels se trouvent à l'emplacement suivant.

Journal	Emplacement par défaut
Journal de démarrage d'agent logiciel	/opt/vmware-appdirector (pour Linux) ou \opt\vmware-appdirector (pour Windows)
Journaux de script de cycle de vie de logiciels	/tmp/taskId (pour Linux) \Users\darwin\AppData\Local\Temp\taskId (pour Windows)

Collection de journaux pour les déploiements distribués

Vous pouvez créer un fichier zip qui regroupe tous les journaux des composants d'un déploiement distribué. .

Restauration d'une installation qui a échoué

En cas d'échec et de restauration d'une installation, l'administrateur système doit vérifier que tous les fichiers requis ont été désinstallés avant de démarrer une autre installation. Certains fichiers doivent être désinstallés manuellement.

Restaurer une installation minimale

Pour désinstaller complètement une installation IaaS vRealize Automation ayant échoué, un administrateur système doit supprimer manuellement certains fichiers et rétablir la base de données.

Procédure

- 1 Si les composants suivants sont présents, désinstallez-les avec le programme de désinstallation de Windows.
 - Agents vRealize Automation
 - DEM-Worker vRealize Automation
 - DEM-Orchestrator vRealize Automation
 - Serveur vRealize Automation Server

- WAPI de vRealize Automation

Note Si le message suivant s'affiche, redémarrez la machine et procédez comme suit :
 Erreur à l'ouverture du fichier journal d'installation. Vérifiez que
 l'emplacement du fichier journal spécifié existe et est inscriptible

Note Si le système Windows a été rétabli ou si vous avez désinstallé IaaS, vous devez exécuter la commande `iisreset` avant de réinstaller l'IaaS de vRealize Automation.

- 2 Rétablissez votre base de données l'état dans laquelle elle se trouvait avant le démarrage de l'installation. La méthode à employer dépend de la méthode d'installation de la base de données originale.
- 3 Dans IIS (Internet Information Services Manager), sélectionnez le site Web par défaut (ou un site personnalisé) et cliquez sur **Liaisons**. Supprimez la liaison https (valeur par défaut 443).
- 4 Vérifiez que le référentiel d'applications, vRealize Automation et le WAPI ont été supprimés et que les pools d'applications RepositoryAppPool, vCACAppPool et WapiAppPool ont été également supprimés.

Résultats

L'installation est complètement supprimée.

Restaurer une installation distribuée

Pour désinstaller complètement une installation IaaS ayant échoué, un administrateur système doit supprimer manuellement certains fichiers et rétablir la base de données.

Procédure

- 1 Si les composants suivants sont présents, désinstallez-les avec le programme de désinstallation de Windows.
 - Serveur vRealize Automation
 - WAPI de vRealize Automation

Note Si le message suivant s'affiche, redémarrez la machine et procédez comme suit :
 Erreur à l'ouverture du fichier journal d'installation. Vérifiez que
 l'emplacement du fichier journal spécifié existe et est inscriptible.

Note Si le système Windows a été rétabli ou si vous avez désinstallé IaaS, vous devez exécuter la commande `iisreset` avant de réinstaller l'IaaS de vRealize Automation.

- 2 Rétablissez votre base de données l'état dans laquelle elle se trouvait avant le démarrage de l'installation. La méthode à employer dépend de la méthode d'installation de la base de données originale.
- 3 Dans IIS (Internet Information Services Manager), sélectionnez le site Web par défaut (ou un site personnalisé) et cliquez sur **Liaisons**. Supprimez la liaison https (valeur par défaut 443).

- 4 Vérifiez que le référentiel d'applications, le vCAC et le WAPI ont été supprimés et que les pools d'applications RepositoryAppPool, vCACAppPool et WapiAppPool ont été également supprimés.

Résultats

Tableau 1-42. Restaurer des points d'échec

Point d'échec	Action
Installation de Manager Service	S'il est présent, désinstallez le serveur vCloud Automation Center.
Installation de DEM-Orchestrator	S'il est présent, désinstallez le DEM Orchestrator.
Installation de DEM-Worker	S'il est présent, désinstallez tous les DEM Workers.
Installation d'un agent	S'il est présent, désinstallez tous les agents vRealize Automation.

Création d'un bundle de support vRealize Automation

Vous pouvez créer un bundle de support vRealize Automation à l'aide de l'interface de gestion du dispositif vRealize Automation. Les bundles de support collectent les journaux et vous permettent, ainsi qu'au support technique de VMware, de résoudre les problèmes de vRealize Automation.

Procédure

- 1 Connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Cliquez sur **vRA > Journaux**.
- 3 Cliquez sur **Créer un bundle de support**.
- 4 Cliquez sur **Télécharger** et enregistrez le fichier du bundle de support sur votre système.

Résultats

Les bundles de support incluent des informations sur le dispositif vRealize Automation et les serveurs Windows IaaS. Si vous perdez la connectivité entre le dispositif vRealize Automation et les composants IaaS, le bundle de support ne dispose peut-être pas des journaux de composant IaaS.

Pour afficher les fichiers journaux collectés, décompressez le bundle de support et ouvrez le fichier `Environment.html` dans un navigateur Web. Sans connectivité, les composants IaaS peuvent s'afficher en rouge dans la table Nœuds. Il se peut également que les journaux IaaS soient manquants du fait que le service vRealize Automation Management Agent s'est arrêté sur les serveurs Windows IaaS qui s'affichent en rouge.

Ligne de commande : pour générer un bundle de support à partir de la ligne de commande du dispositif vRealize Automation en tant qu'utilisateur racine, vous pouvez exécuter `vcac-support` ou `vcac-config log-bundle`.

Vous pouvez également exécuter la commande `log-bundle` complète comme indiqué dans l'exemple suivant. Reportez-vous à [vRealize Automation Notions de base sur l'installation depuis la ligne de commande](#) pour obtenir des informations générales sur l'exécution de `vra-command`.

```
# vra-command execute --node cafe.node.497772175.21500 log-bundle --requestor va-1.mycompany.com

Parent command with id='981e3028-c99b-5c92-1bae-7d2bf5b6aaaa' was created.
Waiting for all child commands to complete...
...
Command execution result:
Command id: 3d64d122-0af1-28dd-b5a5-d932b78b3678
  Type: log-bundle
  Node id: cafe.node.497772175.21500
  Node host: va-1.mycompany.com
  Result: The command was successfully executed.
  Result description: {"path": "/opt/vmware/var/support-bundle/log/
va-1.mycompany.com_cafe.node.497772175.21500-VA.zip"}

Status: COMPLETED
```

Dépannage de l'installation générale

Les rubriques consacrées au dépannage de dispositifs vRealize Automation proposent des solutions à des problèmes potentiels liés à l'installation que vous pourriez rencontrer en utilisant vRealize Automation.

L'installation des mises à niveau échoue avec une erreur de délai d'attente des équilibrages de charge

Une installation ou une mise à niveau de vRealize Automation pour un déploiement distribué avec un équilibrage de charge échoue et renvoie une erreur de service 503 non disponible.

Problème

L'installation ou la mise à niveau échoue, car le paramètre d'expiration de l'équilibrage de charge n'accorde pas suffisamment de temps pour l'exécution de la tâche.

Cause

Un paramètre de délai d'expiration d'équilibrage de charge insuffisant peut entraîner un échec. Vous pouvez corriger le problème en augmentant le paramètre de délai d'expiration de l'équilibrage de charge à 100 secondes ou plus et en réexécutant la tâche.

Solution

- 1 Augmentez la valeur du délai d'expiration de l'équilibrage de charge à au moins 100 secondes.
- 2 Réexécutez l'installation ou la mise à niveau.

Les heures des serveurs ne sont pas synchronisées

Une installation peut échouer lorsque les serveurs de temps IaaS ne sont pas synchronisés avec le dispositif vRealize Automation.

Problème

Vous ne pouvez pas vous connecter après une installation ou l'installation échoue pendant son exécution.

Cause

Les serveurs de temps de tous les serveurs ne sont peut-être pas synchronisés.

Solution

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

- Définissez une source de temps de dispositif vRealize Automation :
 - a Connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.
`https://vrealize-automation-appliance-FQDN:5480`
 - b Sélectionnez **Admin > Paramètres de l'heure** et définissez la source de synchronisation de l'heure.

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

- Pour les serveurs IaaS Windows, consultez [Activer la synchronisation de l'heure sur le serveur Windows](#).

Des pages blanches peuvent apparaître lors de l'utilisation d'Internet Explorer 9 ou 10 sur Windows 7

Lorsque vous utilisez Internet Explorer 9 ou 10 sur Windows 7 et que le mode de compatibilité est activé, certaines pages restent blanches.

Conditions préalables

Assurez-vous que la barre de menus est affichée. Si vous utilisez Internet Explorer 9 ou 10, appuyez sur Alt pour afficher la barre de menus (ou cliquez avec le bouton droit de la souris sur la barre d'adresse, puis sélectionnez **Barre de menus**).

Problème

Lors de l'utilisation d'Internet Explorer 9 ou 10 sur Windows 7, les pages suivantes restent blanches :

- Infrastructure.
- Dossier locataire par défaut sur la page Orchestrator.
- Configuration de serveur sur la page Orchestrator.

Cause

Le problème peut s'expliquer par le fait que le mode de compatibilité est activé. Vous pouvez désactiver le mode de compatibilité pour Internet Explorer en procédant comme suit.

Solution

- 1 Sélectionnez **Outils > Paramètres d'affichage de compatibilité**.
- 2 Décochez **Afficher les sites intranet en mode de compatibilité**.
- 3 Cliquez sur **Fermer**.

Impossible d'établir une relation de confiance pour le canal sécurisé SSL/TLS

Il se peut que le message suivant s'affiche : « Impossible d'établir une relation de confiance pour le canal sécurisé SSL/TLS lors de la mise à niveau des certificats de sécurité pour vCloud Automation Center. »

Problème

Si un problème de certificat se produit avec vcac-config.exe lors de la mise à niveau d'un certificat de sécurité, le message suivant peut s'afficher :

La connexion sous-jacente a été fermée : impossible d'établir une relation de confiance pour le canal sécurisé SSL/TLS.

Vous pouvez obtenir davantage d'informations sur la cause de ce problème en utilisant la procédure suivante.

Solution

- 1 Ouvrez vcac-config.exe.config dans un éditeur de texte, puis localisez l'adresse du référentiel :


```
<add key="repositoryAddress" value="https://IaaS-address:443/repository/" />
```
- 2 Ouvrez Internet Explorer à l'adresse.
- 3 Parcourez tous les messages d'erreur éventuels concernant des problèmes de confiance de certificat.
- 4 Obtenez un rapport de sécurité dans Internet Explorer, puis utilisez-le pour déterminer pourquoi le certificat n'est pas approuvé.

Solution

Si les problèmes persistent, répétez la procédure en recherchant l'adresse devant être enregistrée, l'adresse du point de terminaison que vous avez utilisé pour vous enregistrer avec `vcac-config.exe`.

Se connecter au réseau par le biais d'un serveur proxy

Certains sites peuvent se connecter à Internet par le biais d'un serveur proxy.

Conditions préalables

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

Problème

Votre déploiement ne peut pas se connecter au réseau Internet ouvert. Par exemple, vous ne pouvez pas accéder à des sites Web, des clouds publics que vous pouvez gérer ou des adresses de fournisseurs à partir desquelles vous pouvez télécharger des logiciels ou des mises à jour.

Cause

Votre site se connecte à Internet par le biais d'un serveur proxy.

Solution

- 1 Ouvrez un navigateur Web et accédez à l'URL de l'interface de gestion du dispositif vRealize Automation.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Connectez-vous en tant qu'utilisateur racine, puis cliquez sur **Réseau**.
- 3 Entrez le nom de domaine complet ou l'adresse IP, et le numéro de port du serveur proxy de votre site.
- 4 Si votre serveur proxy nécessite des informations d'identification, entrez le nom d'utilisateur et le mot de passe.
- 5 Cliquez sur **Enregistrer les paramètres**.

Étape suivante

La configuration pour l'utilisation d'un serveur proxy peut affecter l'accès de l'utilisateur à VMware Identity Manager. Pour corriger ce problème, reportez-vous à [Le proxy empêche l'utilisateur de VMware Identity Manager de se connecter](#).

Étapes sur la console pour une configuration de contenu initial

Il existe une solution alternative à l'utilisation de l'interface d'installation de vRealize Automation pour créer le compte de l'administrateur de configuration et le contenu initial.

Au lieu d'utiliser l'interface, entrez des commandes de console pour créer l'utilisateur configurationadmin et le contenu initial. Notez que l'interface peut échouer après exécution d'une partie du processus. Il est donc possible que vous n'ayez besoin que de certaines commandes.

Par exemple, vous pouvez inspecter les journaux et l'exécution du workflow vRealize Orchestrator, puis déterminer que la configuration basée sur l'interface a créé l'utilisateur configurationadmin mais pas le contenu initial. Dans ce cas, vous pouvez entrer seulement les deux dernières commandes de consoles pour terminer le processus.

Problème

Lors de la dernière partie de l'installation de vRealize Automation, vous suivez le processus d'entrée d'un nouveau mot de passe, créez le compte utilisateur local configurationadmin et créez le contenu initial. Une erreur se produit et l'interface entre dans un état non récupérable.

Solution

- 1 Connectez-vous à la console du dispositif vRealize Automation en tant qu'utilisateur racine.
- 2 Importez le workflow vRealize Orchestrator en entrant la commande suivante :

```
/usr/sbin/vcac-config -e content-import --workflow /usr/lib/vcac/tools/initial-config/vra-
initial-config-bundle-workflow.package --user $SSO_ADMIN_USERNAME --password
$SSO_ADMIN_PASSWORD --tenant $TENANT
```

- 3 Exécutez le workflow pour créer l'utilisateur configurationadmin :

```
/usr/bin/python /opt/vmware/share/htdocs/service/wizard/initialcontent/workflowexecutor.py
--host $CURRENT_VA_HOSTNAME --username $SSO_ADMIN_USERNAME --password $SSO_ADMIN_PASSWORD
--workflowid f2b3064a-75ca-4199-a824-1958d9c1efed --configurationAdminPassword
$CONFIGURATIONADMIN_PASSWORD --tenant $TENANT
```

- 4 Pour importer le Blueprint ASD, entrez la commande suivante :

```
/usr/sbin/vcac-config -e content-import --blueprint /usr/lib/vcac/tools/initial-config/
vra-initial-config-bundle-asd.zip --user $CONFIGURATIONADMIN_USERNAME --password
$CONFIGURATIONADMIN_PASSWORD --tenant $TENANT
```

- 5 Exécutez le workflow pour configurer le contenu initial :

```
/usr/bin/python /opt/vmware/share/htdocs/service/wizard/initialcontent/workflowexecutor.py
--host $CURRENT_VA_HOSTNAME --username $SSO_ADMIN_USERNAME --password $SSO_ADMIN_PASSWORD
--workflowid ef00fce2-80ef-4b48-96b5-fdee36981770 --configurationAdminPassword
$CONFIGURATIONADMIN_PASSWORD
```

Impossible de rétrograder les licences de vRealize Automation

Une erreur se produit lorsque vous soumettez la clé de licence d'une édition inférieure du produit.

Problème

Le message suivant s'affiche lors de l'utilisation de la page de gestion des licences de l'interface d'administration de vRealize Automation pour envoyer la clé à une édition de produit inférieure à l'édition actuelle. Par exemple, vous utilisez par une licence d'entreprise et essayez d'entrer une licence avancée.

```
Unable to downgrade existing license edition
```

Cause

Cette version de vRealize Automation ne prend pas en charge la rétrogradation de licences. Vous pouvez uniquement ajouter des licences d'une édition équivalente ou supérieure.

Solution

Pour passer à une édition inférieure, réinstallez vRealize Automation.

Dépannage du dispositif vRealize Automation

Les articles relatifs au dépannage de dispositifs vRealize Automation proposent des solutions aux possibles problèmes liés à l'installation que vous pouvez rencontrer lors de l'utilisation des dispositifs vRealize Automation.

Le téléchargement des programmes d'installation échoue

Le téléchargement des programmes d'installation échouent à partir du dispositif vRealize Automation.

Problème

Les programmes d'installation ne se téléchargent pas lors de l'exécution de `setup__vrealize-automation-appliance-FQDN@5480.exe`.

Cause

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

Solution

- 1 Vérifiez que vous pouvez vous connecter à l'URL vRealize Automation dans un navigateur Web.
`https://vrealize-automation-appliance-FQDN`
- 2 Consultez les autres rubriques de dépannage du dispositif vRealize Automation.
- 3 Téléchargez le fichier de configuration et reconnectez-vous au dispositif vRealize Automation.

Le fichier Encryption.key comporte des autorisations incorrectes

Une erreur système peut survenir si des autorisations incorrectes sont attribuées au fichier Encryption.key pour un dispositif virtuel.

Conditions préalables

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

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

Problème

Vous vous connectez à dispositif vRealize Automation et la page Locataires s'affiche. Une fois que la page a commencé à se charger, le message Erreur système s'affiche.

Cause

Le fichier Encryption.key comporte des autorisations incorrectes ou le niveau de groupe ou d'utilisateur propriétaire est attribué de manière incorrecte.

Solution

- 1 Affichez le fichier journal /var/log/vcac/catalina.out et recherchez le message Cannot write to /etc/vcac/Encryption.key.
- 2 Accédez au répertoire /etc/vcac/ et vérifiez les autorisations et la propriété pour le fichier Encryption.key. Vous devez voir une ligne similaire à la suivante :

```
-rw----- 1 vcac vcac 48 Dec 4 06:48 encryption.key
```

Read and write permission is required and the owner and group for the file must be vcac.

- 3 Si le résultat que vous voyez est différent, modifiez les autorisations et la propriété du fichier si nécessaire.

Étape suivante

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

Échec du démarrage d'Identity Manager pour la gestion des annuaires après le redémarrage de Horizon-Workspace

Dans un environnement vRealize Automation à haute disponibilité, le démarrage d'Identity Manager peut échouer après le redémarrage du service horizon-workspace.

Problème

Le service horizon-workspace ne peut pas démarrer à cause d'une erreur similaire à celle qui suit :

```
Error creating bean with name
'liquibase' defined in class path resource [spring/datastore-wireup.xml]:
Invocation of init method failed; nested exception is
liquibase.exception.LockException: Could not acquire change log lock. Currently
locked by fe80:0:0:0:250:56ff:fea8:7d0c%eth0
(fe80:0:0:0:250:56ff:fea8:7d0c%eth0) since 10/29/15
```

Cause

Identity Manager peut entraîner un échec au démarrage dans un environnement à haute disponibilité à cause de problèmes liés à l'utilitaire de gestion des données de liquibase utilisées par vRealize Automation.

Solution

- 1 Connectez-vous en tant qu'utilisateur racine à une session de console sur le dispositif vRealize Automation.

- 2 Arrêtez le service horizon-workspace en entrant la commande suivante.

```
#service horizon-workspace stop
```

- 3 Ouvrez le shell Postgres en tant que super utilisateur.

```
su postgres
```

- 4 Accédez au répertoire bin correct.

```
cd /opt/vmware/vpostgres/current/bin
```

- 5 Connectez-vous à la base de données.

```
psql vcac
```

- 6 À partir de `saas.databasechangelock`, exécutez la requête SQL suivante.

```
select * from databasechangelock;
```

Si la sortie affiche la valeur « t » pour true, le verrou doit être désactivé manuellement.

- 7 Si vous désactivez manuellement le verrou, exécutez la requête SQL suivante.

```
update saas.databasechangelock set locked=FALSE, lockgranted=NULL, lockedby=NULL where
id=1;
```

- 8 À partir de `saas.databasechangelock`, exécutez la requête SQL suivante.

```
select * from databasechangelock;
```

La sortie devrait afficher une valeur de « f » pour false, cela signifie qu'il est déverrouillé.

9 Quittez la base de données vcac Postgres.

```
vcac=# \q
```

10 Fermez le shell Postgres.

```
exit
```

11 Démarrez le service horizon-workspace.

```
#service horizon-workspace start
```

Attributions de rôles de dispositifs incorrectes après basculement

Après un basculement, les nœuds du dispositif vRealize Automation master et de réplica risquent de ne pas disposer de la bonne attribution de rôles, ce qui affecte tous les services nécessitant un accès en écriture à la base de données.

Problème

Dans un cluster à haute disponibilité de dispositifs vRealize Automation, vous arrêtez le nœud master de la base de données ou le rendez inaccessible. Vous utilisez l'interface de gestion sur un autre nœud pour promouvoir celui-ci au rang de nouveau nœud master, ce qui restaure l'accès en écriture à la base de données vRealize Automation.

Ensuite, vous remettez en ligne l'ancien nœud master, mais l'onglet Cluster dans l'interface de gestion indique toujours que le nœud est le nœud master même s'il ne l'est plus. Les tentatives d'utilisation d'une interface de gestion de nœuds pour résoudre le problème en promouvant officiellement l'ancien nœud au rang de nœud master échouent.

Solution

Lors d'un basculement, suivez ces directives pour configurer les anciens et nouveaux nœuds master.

- Avant de promouvoir un autre nœud au rang de nœud master, retirez le nœud master précédent du pool d'équilibrage de charge des nœuds de dispositifs vRealize Automation.
- Pour que vRealize Automation remplace un ancien nœud master dans le cluster, laissez l'ancienne machine venir en ligne. Ouvrez ensuite l'interface de gestion du nouveau nœud master. Recherchez l'ancien nœud signalé comme `invalid` dans l'onglet Cluster, puis cliquez sur son bouton **Réinitialiser**.

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

- Pour remettre un ancien nœud master dans le cluster, mettez en ligne la machine, puis joignez-la au cluster comme s'il s'agissait d'un nouveau nœud. Lors de la jonction, désignez le nœud récemment promu comme nœud principal.

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

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

Pannes après la promotion de nœuds de réplica et master

Un incident d'espace disque, lié à la promotion de nœuds de base de données de dispositif vRealize Automation de réplica et master, peut provoquer des problèmes de provisionnement.

Problème

Le nœud master n'a plus d'espace disque. Vous vous connectez à sa page de base de données d'interface de gestion, et promouvez un nœud de réplica disposant de suffisamment d'espace pour devenir le nouveau nœud master. La promotion semble réussir lorsque vous actualisez la page d'interface de gestion, même si un message d'erreur s'affiche.

Plus tard, sur le nœud qui était l'ancien nœud master, vous libérez l'espace disque. Cependant, après la repromotion du nœud au rang de master, les opérations de provisionnement échouent et restent bloquées à l'état IN_PROGRESS.

Cause

vRealize Automation ne peut pas correctement mettre à jour l'ancienne configuration de nœud master en présence du problème d'insuffisance d'espace.

Solution

Si l'interface de gestion affiche des erreurs pendant la promotion, excluez temporairement le nœud de l'équilibrage de charge. Corrigez le problème du nœud, en ajoutant par exemple un disque, avant de le réinclure dans l'équilibrage de charge. Ensuite, actualisez la page de base de données de l'interface de gestion et vérifiez que les nœuds appropriés sont les nœuds master et de réplica.

Enregistrements des services composants vRealize Automation incorrects

L'interface de gestion du dispositif vRealize Automation peut vous aider à résoudre des problèmes d'enregistrement avec les services de composants vRealize Automation.

Problème

Dans des conditions normales de fonctionnement, tous les services composants vRealize Automation doit être uniques et dans un état ENREGISTRÉ. Tout autre ensemble de conditions peut entraîner un comportement imprévisible de vRealize Automation.

Cause

Les exemples de problèmes suivants peuvent se produire avec des composants services vRealize Automation.

- Un service est devenu inactif.
- Les paramètres du serveur ont placé le service dans un état autre qu'ENREGISTRÉ.
- Une dépendance sur un autre service a placé le service dans un état autre qu'ENREGISTRÉ.
- Le service SQL peut ne pas être en cours d'exécution.

Solution

Réenregistrez les services de composants qui semblent présenter des problèmes.

- 1 Prenez un snapshot du dispositif vRealize Automation.

Il se peut que vous deviez rétablir le snapshot si vous essayez de différentes modifications de service et que le dispositif finit dans un état imprévisible.

- 2 Connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.

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

- 3 Cliquez sur **Services**.

- 4 Dans la liste de services, recherchez un service qui n'est pas dans l'état approprié ou présente d'autres problèmes.

- 5 Si un service défectueux est `iaas-service`, accédez à l'étape suivante.

Sinon, pour que vRealize Automation enregistre de nouveau le service, connectez-vous à une session de console sur le dispositif vRealize Automation en tant qu'utilisateur racine, puis redémarrez vRealize Automation en entrant la commande suivante.

```
service vcac-server restart
```

Si des services sont associés à l'instance intégrée de vRealize Orchestrator, entrez la commande supplémentaire suivante.

```
service vco-restart restart
```

- 6 Si un service défectueux est `iaas-service`, procédez comme suit pour l'enregistrer de nouveau.

- a N'annulez pas l'enregistrement du service.
- b Sur le serveur Web IaaS principal, connectez-vous avec un compte disposant de droits d'administrateur.
- c Ouvrez une invite de commande en tant qu'administrateur.
- d Exécutez la commande suivante.

```
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterSolutionUser -url https://appliance-or-load-balancer-IP-or-FQDN/ -t
vsphere.local -cu administrator -cp password -f "C:\Program Files (x86)\VMware\vCAC
\Server\Model Manager Data\Cafe\Vcac-Config.data" -v
```

Le mot de passe est le mot de passe administrator@vsphere.local.

- e Exécutez une commande pour mettre à jour les informations d'enregistrement dans la base de données IaaS.

SQL Server avec l'authentification Windows :

```
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
MoveRegistrationDataToDb -s IaaS-SQL-server-IP-or-FQDN -d SQL-database-name -f
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.data" -v
```

SQL Server avec l'authentification SQL native :

```
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
MoveRegistrationDataToDb -s SQL-server-IP-or-FQDN -d SQL-database-name -su SQL-user -
sp SQL-user-password -f "C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data
\Cafe\Vcac-Config.data" -v
```

Pour trouver le nom du serveur ou de la base de données, examinez le fichier suivant dans un éditeur de texte et recherchez repository. Les valeurs Source de données et Catalogue initial contiennent respectivement l'adresse du serveur et le nom de la base de données.

```
C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Web\Web.config
```

L'utilisateur SQL doit disposer de privilèges DBO sur la base de données.

- f Enregistrez les points de terminaison en exécutant les commandes suivantes :

```
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN /vcac
--Endpoint ui -v
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN /WAPI
--Endpoint wapi -v
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN /
repository --Endpoint repo -v
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterEndpoint --EndpointAddress https://IaaS-Web-server-or-load-balancer-IP-or-FQDN /
WAPI/api/status --Endpoint status -v
```

- g Enregistrez les éléments du catalogue en exécutant la commande suivante :

```
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterCatalogTypesAsync -v
```

- h Redémarrez IIS.

```
iisreset
```

- i Connectez-vous à l'hôte principal de IaaS Manager Service.
- j Redémarrez le service Windows vRealize Automation.

```
VMware vCloud Automation Center Service
```

- 7 Pour réenregistrer des services associés à un système externe, par exemple une instance externe de vRealize Orchestrator, connectez-vous au système externe et redémarrez-y les services.

La carte réseau supplémentaire provoque des erreurs d'interface de gestion

Après avoir ajouté une deuxième carte d'interface réseau à un dispositif vRealize Automation, certaines pages de l'interface de gestion vRealize Automation échouent à se charger correctement.

Problème

Vous ajoutez une deuxième carte réseau à l'aide de vCenter et les pages suivantes de l'interface de gestion vRealize Automation affichent des erreurs au lieu de se charger.

- La page **État > du réseau** affiche une erreur relative à un script qui ne répond pas.
- La page **Adresse > du réseau** affiche une erreur relative à l'échec de la lecture des informations de l'interface réseau.

Cause

Depuis la version 7.3, le dispositif vRealize Automation peut prendre en charge deux cartes réseau. Toutefois, le modèle d'ingénierie sur lequel repose le dispositif empêche l'interface de gestion de fonctionner correctement tant que vous n'appliquez pas la solution.

Solution

Après avoir ajouté une carte réseau supplémentaire, redémarrez le dispositif vRealize Automation.

Impossible de promouvoir un dispositif virtuel secondaire au rang de dispositif master

Dans vRealize Automation, une faible capacité de mémoire de dispositif virtuel peut empêcher les promotions de dispositif virtuel dans le cluster.

Problème

Le nœud master n'a presque plus de mémoire. Vous vous connectez à sa page de base de données d'interface de gestion et essayez de promouvoir un nœud secondaire au rang de nouveau nœud master. L'erreur suivante se produit.

```
Fail to execute on Node node-name, host is master-FQDN
because of: Could not read remote lock command result for node: node-name
on address: master-FQDN, reason is: 500 Internal Server Error
```

Cause

La promotion ne réussit que lorsque tous les nœuds peuvent confirmer la reconfiguration de cette promotion. La faible capacité mémoire empêche l'ancien nœud master de confirmer, même si tous les nœuds sont accessibles.

Solution

Mettez hors tension le nœud master disposant d'une mémoire insuffisante. Connectez-vous à la page de base de données de l'interface de gestion du nœud secondaire, puis procédez à la promotion de ce dernier.

La durée de rétention du journal de synchronisation Active Directory est trop courte

Dans vRealize Automation, les journaux de synchronisation Active Directory ne remontent que de quelques jours.

Problème

Après deux jours, les journaux de synchronisation Active Directory disparaissent de l'interface de gestion. Les dossiers des journaux disparaissent également à partir du répertoire du dispositif vRealize Automation suivant.

```
/db/elasticsearch/horizon/nodes/0/indices
```

Cause

Pour économiser de l'espace, vRealize Automation définit la durée de rétention maximale pour les journaux de la synchronisation Active Directory à trois jours.

Solution

- 1 Connectez-vous à une session de console sur le dispositif vRealize Automation en tant qu'utilisateur racine.
- 2 Ouvrez le fichier suivant dans un éditeur de texte.
`/usr/local/horizon/conf/runtime-config.properties`
- 3 Augmentez la propriété `analytics.maxQueryDays`.
- 4 Enregistrez et fermez `runtime-config.properties`.
- 5 Redémarrez le Gestionnaire d'identité et les services de recherche élastique.

```
service horizon-workspace restart
service elasticsearch restart
```

RabbitMQ ne parvient pas à résoudre les noms d'hôte

RabbitMQ utilise des noms d'hôte courts pour les dispositifs vRealize Automation par défaut, ce qui risque d'empêcher les nœuds de s'identifier entre eux.

Problème

Vous tentez de joindre un autre dispositif vRealize Automation au cluster et une erreur semblable à l'erreur suivante se produit.

```
Clustering node 'rabbit@sc2-rdops-vm01-dhcp-62-2' with rabbit@company ...
Error: unable to connect to nodes [rabbit@company]: nodedown

DIAGNOSTICS
=====

attempted to contact: [rabbit@company]

rabbit@company:
* unable to connect to epmd (port 4369) on company: nxdomain (non-existing domain)

current node details:
- node name: 'rabbitmq-cli-11@sc2-rdops-vm01-dhcp-62-2'
- home dir: /var/lib/rabbitmq
- cookie hash: 4+kP1tKnxGYaGjrPL2C8bQ==

[2017-09-01 14:58:04] [root] [INFO] RabbitMQ join failed with exit code: 69, see RabbitMQ logs for details.
```

Cause

Votre configuration réseau ne permet pas aux dispositifs vRealize Automation de s'identifier entre eux via un nom d'hôte court.

Solution

- 1 Pour tous les dispositifs vRealize Automation du déploiement, connectez-vous en tant qu'utilisateur racine dans une session de console.

- 2 Arrêtez le service RabbitMQ.

```
service rabbitmq-server stop
```

- 3 Ouvrez le fichier suivant dans un éditeur de texte.

```
/etc/rabbitmq/rabbitmq-env.conf
```

- 4 Définissez la propriété suivante sur true.

```
USE_LONGNAME=true
```

- 5 Enregistrez et fermez rabbitmq-env.conf.

- 6 Réinitialisez RabbitMQ.

```
vcac-vami rabbitmq-cluster-config reset-rabbitmq-node
```

- 7 Sur un seul nœud de dispositif vRealize Automation, exécutez le script suivant.

```
vcac-config cluster-config-ping-nodes --services rabbitmq-server
```

- 8 Sur tous les nœuds, vérifiez que le service RabbitMQ est démarré.

```
vcac-vami rabbitmq-cluster-config get-rabbitmq-status
```

Dépannage des composants IaaS

Les rubriques consacrées au dépannage de composants IaaS vRealize Automation proposent des solutions à des problèmes potentiels liés à l'installation que vous pourriez rencontrer en utilisant vRealize Automation.

Les connexions du coordinateur de transaction distribué sont refusées

Les paramètres d'appel de procédure distante (RPC, Remote Procedure Call) Microsoft peuvent affecter le coordinateur de transactions distribuées (DTC, Distributed Transaction Coordinator) dans vRealize Automation.

Problème

Des erreurs se produisent, indiquant que les connexions DTC entre les serveurs Windows IaaS ou le serveur de base de données SQL vRealize Automation sont refusées.

Cause

Un paramètre de connexion RPC limite l'accès et doit être désactivé.

Solution

Sur tous les serveurs Windows IaaS et sur le serveur de base de données SQL vRealize Automation, supprimez la clé de registre suivante ou définissez-la sur zéro.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\RPC\RestrictRemoteClients
```

Le programme de correction des conditions préalables ne peut pas installer les fonctionnalités .NET

L'option de **correction** du programme de vérification des conditions préalables de vRealize Automation échoue et affiche des messages indiquant que la source d'installation de .NET 3.5.1 est introuvable.

Problème

Le programme de vérification des conditions préalables doit vérifier que .NET 3.5.1 est installé afin de satisfaire aux conditions requises des systèmes Windows Server 2008 R2 avec IIS 7.5 et des systèmes Windows Server 2012 R2 avec IIS 8.

Cause

Pour Windows Server 2012 R2, l'impossibilité de se connecter à Internet peut empêcher l'installation automatique de .NET. Certaines mises à jour de Windows 2012 R2 peuvent également empêcher l'installation. Le problème survient car la version de Windows ne dispose pas d'une copie locale de la source d'installation de .NET Framework 3.5.

Solution

Fournissez manuellement une source d'installation pour .NET Framework 3.5.

- 1 Sur l'hôte Windows, montez une image ISO du support d'installation de Windows Server 2012 R2.
- 2 Dans le gestionnaire de serveur, activez .NET Framework 3.5 à l'aide de l'assistant Ajouter des rôles et des fonctionnalités.
- 3 Pendant l'exécution de l'assistant, accédez au chemin d'installation de .NET Framework 3.5 sur le support ISO.
- 4 Après l'ajout de .NET Framework 3.5, exécutez à nouveau le programme de vérification des conditions préalables de vRealize Automation.

Validation des certificats de serveur pour IaaS

Vous pouvez utiliser la commande `vcac-Config.exe` pour vérifier qu'un serveur IaaS accepte le dispositif vRealize Automation et les certificats du dispositif SSO.

Problème

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

Cause

Des erreurs d'autorisation peuvent se produire lorsque IaaS ne reconnaît pas les certificats de sécurité d'autres composants.

Solution

- 1 Ouvrez une invite de commande en tant qu'administrateur et accédez au répertoire Cafe à l'adresse `vra-installation-dir\Server\Model Manager Data\Cafe`, en général `C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe`.
- 2 Tapez une commande sous la forme de
`Vcac-Config.exe CheckServerCertificates -d [vra-database] -s [vRA SQL server] -v.`
 Les paramètres facultatifs sont `-su [SQL user name]` et `-sp [password]`.

Si la commande s'exécute avec succès, le message suivant s'affiche :

```
Certificates validated successfully.
Command succeeded.
```

Si la commande échoue, un message d'erreur détaillé s'affiche.

Note Cette commande est uniquement disponible sur le nœud du composant Model Manager Data.

Erreur d'informations d'identification lors de l'exécution du programme d'installation d'IaaS

Lorsque vous installez des composants IaaS, vous recevez un message d'erreur au moment de saisir vos informations d'identification de dispositif virtuel.

Problème

Après avoir fourni les informations d'identification au programme d'installation d'IaaS, un message d'erreur `org.xml.sax.SAXParseException` s'affiche.

Cause

Vous avez utilisé des informations d'identification incorrectes ou un format d'informations d'identification incorrect.

Solution

- ◆ Vérifiez que vous utilisez les valeurs de locataire et de nom d'utilisateur corrects.
Par exemple, le locataire SSO par défaut utilise comme nom de domaine `vsphere.local` et non `administrator@vsphere.local`.

Un avertissement d'enregistrement des paramètres s'affiche lors de l'installation d'IaaS

Un message s'affiche lors de l'installation d'IaaS. `Warning: Could not save settings to the virtual appliance during IaaS installation.`

Problème

Un message d'erreur inapproprié indiquant que les paramètres utilisateur n'ont pas été enregistrés s'affiche lors de l'installation d'IaaS.

Cause

Des problèmes de communication ou de réseau peuvent entraîner l'affichage erroné de ce message.

Solution

Ignorez ce message d'erreur et poursuivez l'installation. Ce message ne devrait pas l'échec de la configuration.

Échec de l'installation du serveur de site Web et des Distributed Execution Managers

Votre installation du serveur de site Web et des DEM d'infrastructure du dispositif vRealize Automation ne peut pas se poursuivre si le mot de passe de votre compte de service IaaS contient des guillemets.

Problème

Un message s'affiche vous informant que l'installation des DEM distribués et du serveur de site Web du dispositif vRealize Automation a échoué en raison de paramètres `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 ou entre les dispositifs. Une tentative de connexion échoue en raison d'une absence de réponse ou de l'impossibilité d'établir une connexion.
- Problèmes de certificat approuvé dans IaaS lors de l'utilisation d'une configuration distribuée.
- Incompatibilité de nom de certificat dans une configuration distribuée.

- Le certificat peut être non valide ou il peut exister une erreur dans la chaîne de certificat.
- Le service du référentiel échoue à démarrer.
- Configuration incorrecte de l'équilibrage de charge dans un environnement distribué.

Solution

◆ Connectivité

Vérifiez que vous pouvez vous connecter à l'URL vRealize Automation dans un navigateur Web.

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

◆ Problèmes de certificat approuvé

- Dans IaaS, ouvrez Microsoft Management Console avec la commande `mmc.exe` et vérifiez que le certificat utilisé dans l'installation a été ajouté au magasin de certificats racines de confiance dans la machine.
- Dans un navigateur Web, vérifiez l'état du service MetaModel et assurez-vous qu'aucune erreur de certificat ne s'affiche :

`https://FQDN-or-IP/repository/data/MetaModel.svc`

◆ Incompatibilité de nom de certificat

Cette erreur peut se produire lorsque le certificat est émis à un nom en particulier et qu'un nom ou une adresse IP différente est utilisée. Vous pouvez supprimer l'erreur d'incompatibilité de nom de certificat au cours de l'installation en sélectionnant **Supprimer les incompatibilités de certificat**.

Vous pouvez utiliser également l'option Supprimer les incompatibilités de certificat pour ignorer les erreurs de correspondance de liste à distance de révocation de certificat.

◆ Certificat non valide

Ouvrez la console de gestion Microsoft avec la commande `mmc.exe`. Vérifiez que le certificat n'a pas expiré et que l'état est correct. Procédez ainsi avec tous les certificats de la chaîne de certificats. Vous pouvez avoir à importer d'autres certificats de la chaîne dans le magasin de certificats racine approuvés lors de l'utilisation d'une hiérarchie de certificats.

◆ Service de référentiel

Utilisez les actions suivantes pour vérifier l'état du service du référentiel.

- Dans un navigateur Web, vérifiez l'état du service MetaModel :
`https://FQDN-or-IP/repository/data/MetaModel.svc`
- Vérifiez le fichier `Repository.log` pour consulter les erreurs.
- Réinitialisez l'IIS (`iisreset`) si vous rencontrez des problèmes avec les applications hébergées sur le site Web (Référentiel, vRealize Automation ou WAPI).

- Vérifiez que le site Web se connecte à `%SystemDrive%\inetpub\logs\LogFiles` pour obtenir des informations supplémentaires sur la connexion.
- Vérifiez que l'outil de vérification des conditions préalables s'exécute correctement lors de la vérification des conditions requises.
- Dans Windows 2012, vérifiez que WCF Services sous .NET Framework est installé et que l'activation HTTP est installée.

Les serveurs Windows IaaS ne prennent pas en charge la norme FIPS

Une installation ne peut pas réussir lorsque la norme Information Processing Standard (FIPS) est activée.

Problème

L'installation échoue et renvoie l'erreur suivante pendant l'installation du composant Web IaaS.

Cette implémentation ne fait pas partie des algorithmes de chiffrement validés Windows Platform FIPS.

Cause

vRealize Automation IaaS est basé sur Microsoft Windows Communication Foundation (WCF) qui ne prend pas en charge la norme FIPS.

Solution

Sur le serveur Windows IaaS, désactivez la stratégie FIPS.

- 1 Accédez à **Démarrer > Panneau de configuration > Outils d'administration > Stratégie de sécurité locale**.
- 2 Dans la boîte de dialogue Stratégie de groupe, sous **Stratégies locales**, sélectionnez **Options de sécurité**.
- 3 Trouvez et désactivez l'entrée suivante.

Cryptographie système : utilisez des algorithmes compatibles FIPS pour le cryptage, le hachage et la signature.

L'ajout d'un point de terminaison XaaS génère une erreur interne

Lorsque vous tentez de créer un point de terminaison XaaS, un message d'erreur interne apparaît.

Problème

La création d'un point de terminaison échoue avec le message d'erreur interne suivant : Une erreur interne s'est produite. Si ce problème persiste, contactez votre administrateur système. Lorsque vous contactez votre administrateur système, utilisez la référence `c0DD0C01`. Les codes de référence sont générés de manière aléatoire et ne sont pas liés à un message d'erreur en particulier.

Solution

- 1 Ouvrez le fichier journal du dispositif vRealize Automation.
`/var/log/vcac/catalina.out`
- 2 Localisez le code de référence dans le message d'erreur.
Par exemple, `cODD0C01`.
- 3 Recherchez le code de référence dans le fichier journal pour localiser l'entrée associée.
- 4 Passez en revue les entrées qui apparaissent au-dessus et en dessous de l'entrée associée pour résoudre le problème.

L'entrée de journal associé n'appelle pas spécifiquement la source du problème.

Échec de la désinstallation de l'agent proxy

La suppression d'un agent proxy peut échouer si la journalisation du programme d'installation de Windows est activée.

Problème

Lorsque vous essayez de désinstaller un agent proxy dans le Panneau de configuration Windows, l'opération échoue et l'erreur suivante s'affiche :

Error opening installation log file. Verify that the specified log file location exists and is writable

Cause

Cela peut se produire si la journalisation du programme d'installation de Windows est activée, mais le moteur du programme d'installation de Windows ne peut pas écrire correctement sur le fichier journal de désinstallation. Pour plus d'informations, reportez-vous à [Article 2564571 de la base de connaissances Microsoft](#).

Solution

- 1 Redémarrez votre machine ou 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 Coordinator) de Microsoft sont désactivées sur des machines serveurs Windows.

Problème

Si vous provisionnez une machine alors que les transactions distantes sont désactivées sur le portail Model Manager ou le serveur SQL Server, la demande n'aboutit pas. La collecte de données échoue et la demande de la machine reste à l'état de workflows de clone.

Cause

Les transactions distantes DTC sont désactivées dans l'instance SQL IaaS utilisée par le système vRealize Automation.

Solution

- 1 Lancez Windows Server Manager pour activer DTC sur tous les serveurs vRealize et serveurs SQL associés.

Dans Windows 7, accédez à **Démarrer > Outils d'administration > Services composants**.

Note Vérifiez que tous les serveurs Windows disposent de SID uniques pour la configuration de MSDTC.

- 2 Ouvrez tous les nœuds pour rechercher le DTC local ou le DTC en cluster si vous utilisez un système en cluster.

Accédez à **Services composants > Ordinateurs > Mon ordinateur > Coordinateur de transaction distribué**.

- 3 Cliquez avec le bouton droit sur le DTC local ou en cluster DTC et sélectionnez **Propriétés**.
- 4 Cliquez sur l'onglet **Sécurité**.
- 5 Sélectionnez l'option **Accès DTC réseau**.
- 6 Sélectionnez les options **Autoriser le client distant** et **Autoriser l'administration à distance**.
- 7 Sélectionnez les options **Autoriser l'accès entrant** et **Autoriser l'accès sortant**.
- 8 Entrez ou sélectionnez NT AUTHORITY\Network Service dans le champ **Compte** du Compte d'ouverture de session DTC.
- 9 Cliquez sur **OK**.
- 10 Supprimez les machines bloquées à l'état Workflow de clone.
 - a Connectez-vous à l'interface du produit vRealize Automation.
<https://vrealize-automation-appliance-FQDN/vcac/org/tenant-name>
 - b Accédez à **Infrastructure > Machines gérées**.
 - c Cliquez avec le bouton droit sur la machine cible.
 - d Sélectionnez **Supprimer** pour supprimer la machine.

Erreur dans la communication de Manager Service

Les serveurs IaaS clonés à partir d'un modèle dans lequel DTC a déjà été installé contiennent des identifiants dupliqués pour DTC, ce qui empêche la communication entre les nœuds.

Problème

Le service de gestion IaaS échoue et affiche l'erreur suivante dans le journal de Manager Service.

```
La communication avec le gestionnaire de transaction sous-jacent a échoué. --->
System.Runtime.InteropServices.COMException : le gestionnaire d'action MSDTC n'a pas réussi à
extraire la transaction du gestionnaire de transaction source à cause de problèmes de communication.
Causes possibles : un pare-feu est présent et il ne présente pas d'exception pour la procédure MSDTC,
les deux machines ne se trouvent pas avec leur nom NetBIOS ou la prise en charge des transactions de
réseau n'est pas activée pour l'un des gestionnaires de transactions.
```

Cause

Lorsque vous clonez un serveur IaaS sur lequel DTC est déjà installé, le clone contient le même identifiant unique pour DTC que le parent. Échec de la communication entre les deux machines.

Solution

- 1 Sur le clone, ouvrez une invite de commande en tant qu'administrateur.
- 2 Exécutez la commande suivante.

```
msdtc -uninstall
```

- 3 Redémarrez le clone.
- 4 Ouvrez une autre invite de commande et exécutez la commande suivante.

```
msdtc -install manager-service-host-FQDN
```

Le comportement de personnalisation des e-mails a été modifié

Dans vRealize Automation 6.0 ou version ultérieure, seules les notifications générées par le composant IaaS peuvent être personnalisées à l'aide de la fonctionnalité du modèle d'e-mail des versions antérieures.

Solution

Vous pouvez utiliser les modèles XSLT suivants :

- ArchivePeriodExpired
- EpiRegister
- EpiUnregister
- LeaseAboutToExpire
- LeaseExpired
- LeaseExpiredPowerOff
- ManagerLeaseAboutToExpire
- ManagerLeaseExpired
- ManagerReclamationExpiredLeaseModified

- ManagerReclamationForcedLeaseModified
- ReclamationExpiredLeaseModified
- ReclamationForcedLeaseModified
- VdiRegister
- VdiUnregister

Les modèles d'e-mail se trouvent dans le répertoire `\Templates` sous le répertoire d'installation du serveur, généralement `%SystemDrive%\Program Files x86\VMware\vCAC\Server`. Le répertoire `\Templates` contient également des modèles XSLT qui ne sont plus pris en charge et ne peuvent pas être modifiés.

Dépannage des erreurs de connexion

Les rubriques consacrées au dépannage des erreurs de connexion pour vRealize Automation proposent des solutions à des problèmes potentiels liés à l'installation que vous pourriez rencontrer en utilisant vRealize Automation.

Des tentatives de connexion en tant qu'administrateur IaaS avec des informations d'identification au format UPN incorrect échouent sans explication

Vous tentez de vous connecter à vRealize Automation en tant qu'administrateur IaaS et vous êtes redirigé sur la page de connexion sans explication.

Problème

Si vous tentez de vous connecter à vRealize Automation en tant qu'administrateur IaaS avec des informations d'identification UPN qui n'incluent pas la partie *@ votredomaine* du nom d'utilisateur, vous êtes immédiatement déconnecté de SSO et redirigé vers la page de connexion sans explication.

Cause

L'UPN entré doit respecter le format *yourname.admin@yourdomain*, par exemple si vous vous connectez en utilisant *jsmith.admin@sqa.local* comme nom d'utilisateur alors que l'UPN dans Active Directory est défini sur *jsmith.admin*, la connexion échoue.

Solution

Pour corriger le problème, modifiez la valeur `userPrincipalName` pour inclure le contenu *@yourdomain* requis et réessayez. Dans cet exemple, le nom UPN doit être *jsmith.admin@sqa.local*. Cette information est fournie dans le fichier journal du dossier `log/vcac`.

La connexion échoue avec la haute disponibilité

Lorsque vous utilisez plusieurs dispositifs vRealize Automation, ceux-ci doivent pouvoir s'identifier entre eux par un nom d'hôte court. Sinon, vous ne pouvez pas vous connecter.

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

Problème

Vous configurez vRealize Automation pour la haute disponibilité en installant un dispositif vRealize Automation supplémentaire. Lorsque vous tentez de vous connecter à vRealize Automation, un message sur une licence non valide s'affiche. Le message est toutefois incorrect, car vous avez déterminé que votre licence est valide.

Cause

Les nœuds du dispositif vRealize Automation ne forment pas correctement un cluster à haute disponibilité tant qu'ils ne peuvent pas résoudre les noms d'hôtes courts des nœuds du cluster.

Solution

- ◆ Modifiez ou créez une ligne de recherche dans `/etc/resolv.conf`. La ligne doit inclure les domaines qui contiennent les dispositifs vRealize Automation. Quand il y a plusieurs domaines, séparez-les par des espaces. Par exemple :

```
search sales.mycompany.com support.mycompany.com
```

- ◆ Modifiez ou créez des lignes de domaine dans `/etc/resolv.conf`. Chaque ligne doit inclure un domaine qui contient des dispositifs vRealize Automation. Par exemple :

```
domain support.mycompany.com
```

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

```
node1    node1.support.mycompany.com
node2    node2.support.mycompany.com
```

Le proxy empêche l'utilisateur de VMware Identity Manager de se connecter

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

Conditions préalables

Configurez vRealize Automation pour accéder au réseau via un serveur de proxy. Reportez-vous à [Se connecter au réseau par le biais d'un serveur proxy](#).

Problème

Vous configurez vRealize Automation pour accéder au réseau via un serveur de proxy, et les utilisateurs de VMware Identity Manager voient l'erreur suivante lorsqu'ils tentent de se connecter.

Error Unable to get metadata

Solution

1 Connectez-vous à la console du dispositif vRealize Automation en tant qu'utilisateur racine.

2 Ouvrez le fichier suivant dans un éditeur de texte.

```
/etc/sysconfig/proxy
```

3 Mettez à jour la ligne NO_PROXY afin d'ignorer le serveur de proxy pour les connexions VMware Identity Manager.

```
NO_PROXY=vrealize-automation-hostname
```

Par exemple : NO_PROXY="localhost, 127.0.0.1, automation.mycompany.com"

4 Enregistrez et fermez le proxy.

5 Redémarrez le service Horizon Workspace en saisissant la commande suivante.

```
service horizon-workspace restart
```

Mise à niveau et migration de vRealize Automation

Vous pouvez mettre à niveau votre environnement vRealize Automation actuel vers la dernière version.

Mise à niveau sur place et mise à niveau en parallèle

Selon votre environnement vRealize Automation actuel, vous pouvez procéder à une mise à niveau vers la dernière version en effectuant une mise à niveau sur place ou une mise à niveau en parallèle. Examinez les informations sur cette page pour déterminer la meilleure méthode de mise à niveau pour votre environnement.

Une mise à niveau sur place est un processus en plusieurs étapes. Vous effectuez les procédures dans un ordre particulier pour mettre à jour les divers composants de votre environnement actuel. Vous devez mettre à niveau tous les composants du produit vers la même version. Vous pouvez uniquement effectuer une mise à niveau sur place pour ces chemins d'accès.

- vRealize Automation 6.2.5 vers 7.5
- vRealize Automation 7.1.x vers la version 7.5
- vRealize Automation 7.2.x vers la version 7.5
- vRealize Automation 7.3.x vers la version 7.5
- vRealize Automation 7.4.x vers la version 7.5

Une mise à niveau côte-à-côte migre les données de votre environnement vRealize Automation actuel vers un environnement cible déployé avec la version de vRealize Automation la plus récente. Vous pouvez effectuer une mise à niveau en parallèle pour ces chemins d'accès.

- vRealize Automation 6.2.0 à 6.2.5 vers la version 7.5
- vRealize Automation 7.0 et 7.0.1 vers la version 7.5

■ vRealize Automation 7.1.x, 7.2.x, 7.3.x, 7.4.x vers la version 7.5

La migration ne modifie pas votre environnement actuel. Si votre environnement actuel est intégré à vCloud Director ou à vCloud Air, ou s'il dispose de points de terminaison physiques, vous devez utiliser la migration pour effectuer une mise à niveau. La migration supprime tous les points de terminaison non pris en charge, ainsi que tout ce qui leur est associé dans l'environnement cible.

Recherchez votre version de vRealize Automation dans le tableau. Utilisez les documents situés à droite pour effectuer une mise à niveau de votre environnement vRealize Automation vers la version la plus récente.

Tableau 1-43. Chemins de mise à niveau pris en charge vers la version actuelle de vRealize Automation

Votre version installée actuellement	Documentation pour les mises à niveau progressives
vRealize Automation 7.1.x, 7.2.x, 7.3.x et 7.4.x	Reportez-vous à l'une des sections suivantes. <ul style="list-style-type: none"> ■ Mise à niveau de vRealize Automation 7.1 ou version ultérieure vers la version 7.5 ■ Migration de vRealize Automation
vRealize Automation 7.0 ou 7.0.1	Reportez-vous à Migration de vRealize Automation .
vRealize Automation 6.2.5	Reportez-vous à l'une des sections suivantes. <ul style="list-style-type: none"> ■ Mise à niveau de vRealize Automation 6.2.5 vers la version 7.5 ■ Migration de vRealize Automation
vRealize Automation 6.2.0, 6.2.1, 6.2.2, 6.2.3, 6.2.4	Reportez-vous à Migration de vRealize Automation

Ce tableau fournit des informations sur la mise à niveau à partir d'une version antérieure de vCloud Automation Center. Vous devez effectuer la mise à niveau vers vRealize Automation 6.2.5 avant d'effectuer la mise à niveau vers la dernière version de vRealize Automation. Vous pouvez trouver des liens vers la documentation de toutes les versions 5.x et 6.x de vCloud Automation Center et de vRealize Automation à l'adresse <https://www.vmware.com/support/pubs/vcac-pubs.html>.

Tableau 1-44. Chemins de mise à niveau pris en charge vers vRealize Automation 6.2.5

Votre version installée actuellement	Documentation pour les mises à niveau progressives
vCloud Automation Center 6.0	Effectuez les mises à niveau dans l'ordre suivant : <ol style="list-style-type: none"> 1 <i>Mise à niveau de vCloud Automation Center de la version 6.0 vers la version 6.0.1</i> 2 <i>Mise à niveau vers vCloud Automation Center 6.1</i> 3 <i>Mise à niveau vers vRealize Automation 6.2.x</i>
vCloud Automation Center 6.0.1	Effectuez les mises à niveau dans l'ordre suivant : <ol style="list-style-type: none"> 1 <i>Mise à niveau vers vCloud Automation Center 6.1</i> 2 <i>Mise à niveau vers vRealize Automation 6.2.x</i>

Tableau 1-44. Chemins de mise à niveau pris en charge vers vRealize Automation 6.2.5 (suite)

Votre version installée actuellement	Documentation pour les mises à niveau progressives
vCloud Automation Center 6.1.x	<i>Mise à niveau vers vRealize Automation 6.2.x</i>
vRealize Automation 6.2.x	Mettez directement à niveau vers la version 6.2.5, comme décrit dans la section <i>Mise à niveau vers vRealize Automation 6.2.x</i>

Note vCloud Automation Center a été renommé vRealize Automation dans la version 6.2.0. Seuls l'interface utilisateur et les noms de services ont été modifiés. Les noms de répertoires et de programmes contenant vcac ne sont pas affectés.

Si vous mettez à niveau un environnement 6.2.x, vérifiez ces éléments.

- L'outil assistant de mise à jour de test de production VMware vRealize analyse votre environnement vRealize Automation 6.2.x, recherche les configurations de fonctionnalités qui peuvent entraîner des problèmes de mise à niveau et vérifie que votre environnement est prêt pour la mise à niveau. Pour télécharger cet outil et la documentation associée, accédez à la page de téléchargement du produit [Outil de test de production VMware vRealize](#).
- La mise à niveau d'un environnement 6.2.x vers la dernière version de vRealize Automation introduit plusieurs modifications fonctionnelles. Pour plus d'informations, reportez-vous à [Remarques relatives à la mise à niveau vers cette version de vRealize Automation](#).
- Si vous avez personnalisé votre déploiement de vRealize Automation 6.2.x, contactez l'équipe d'assistance CCE locale pour obtenir des informations supplémentaires sur les considérations de mise à niveau.
- Les contrôles du dictionnaire de propriétés qui ne sont pas pris en charge après la mise à niveau peuvent être restaurés à l'aide de vRealize Orchestrator et de relations de dictionnaire de propriétés.
- Si des workflows dans votre environnement source contiennent du code obsolète, reportez-vous à *vRealize Automation Extensibility Migration Guide* pour obtenir des informations sur les modifications du code requises pour la conversion en abonnements aux événements du broker. Ce document est disponible dans la section *Pour en savoir plus sur vRealize Automation* de la [documentation du produit vRealize Automation](#).

Pour éviter tout problème connu lors de la mise à niveau de vRealize Automation 6.2.0, exécutez les étapes suivantes sur chaque nœud de site Web IaaS avant de procéder à la mise à niveau. Ce problème affecte la version 6.2.0 uniquement. Les autres versions 6.2.x ne sont pas concernées.

- 1 Ouvrez le Bloc-Notes avec les droits d'administration. Dans Démarrer, cliquez avec le bouton droit sur l'icône du Bloc-notes et sélectionnez **Exécuter en tant qu'administrateur**.
- 2 Ouvrez la ligne suivante :
`C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Web\web.config`
- 3 Localisez l'instruction suivante dans le fichier :

```
<!-- add key="DisableMessageSignatureCheck" value="false"-->
```

- 4 Supprimez le commentaire de l'instruction et modifiez la valeur false en true.

```
<add key="DisableMessageSignatureCheck" value="true" />
```

- 5 Enregistrez le fichier.

Si le Bloc-Notes vous invite à Enregistrer sous, cela signifie que vous ne l'avez pas ouvert en tant qu'administrateur. Il vous faut donc revenir à l'étape 1.

- 6 Ouvrez une invite de commande avec des droits d'administration. Dans Démarrer, cliquez avec le bouton droit sur l'icône de l'invite de commande et sélectionnez **Exécuter en tant qu'administrateur**.
- 7 Exécutez une réinitialisation.
- 8 Répétez les étapes 1 à 7 pour tous les nœuds de site Web.

Mise à niveau de vRealize Automation 7.1 ou version ultérieure vers la version 7.5

Lorsque vous mettez à niveau votre environnement vRealize Automation 7.1 ou version ultérieure vers la version 7.5, vous utilisez des procédures de mise à niveau spécifiques à l'environnement 7.1 ou version ultérieure.

Ces informations sont spécifiques à la mise à niveau de vRealize Automation 7.1 ou version ultérieure vers la version 7.5. Pour obtenir des informations sur les autres chemins de mise à niveau pris en charge, reportez-vous à la section [Mise à niveau et migration de vRealize Automation](#).

Mise à niveau depuis vRealize Automation 7.1.x

Vous pouvez mettre à niveau vRealize Automation 7.1.x vers cette version de vRealize Automation. Vous utilisez des procédures de mise à niveau spécifiques à cette version pour mettre à niveau votre environnement.

Une mise à niveau sur place est un processus en trois étapes. Vous mettez à niveau les composants de votre environnement actuel dans l'ordre suivant.

- 1 Dispositif vRealize Automation
- 2 Serveur Web IaaS
- 3 Migrer vRealize Orchestrator

Vous devez mettre à niveau tous les composants du produit vers la même version.

À partir de vRealize Automation 7.2, JFrog Artifactory Pro n'est plus inclus avec le dispositif vRealize Automation. Si vous procédez à une mise à niveau d'une version antérieure de vRealize Automation, le processus de mise à niveau supprime JFrog Artifactory Pro. Pour plus d'informations, reportez-vous à [l'article 2147237 de la base de connaissances](#).

Pendant la mise à niveau, les modifications existantes des tailles maximales des chaînes et des messages dans `managerservice.exe.config` sont réinitialisées à leurs valeurs par défaut : `<binding name="ProxAgentBinding" maxReceivedMessageSize="13107200">` et `<readerQuotas maxStringContentLength="13107200" />`. Avant de procéder à la mise à niveau, enregistrez les valeurs de ces chaînes et modifiez-les en conséquence après la mise à niveau.

Conditions préalables pour la mise à niveau de vRealize Automation

Avant de démarrer le processus de mise à niveau de vRealize Automation, passez en revue les conditions préalables ci-dessous.

Conditions requises de la configuration système

Vérifiez que les conditions préalables suivantes sont réunies avant de commencer une mise à niveau.

- Vérifiez que tous les dispositifs et serveurs faisant partie de votre déploiement respectent la configuration système requise pour la dernière version. Reportez-vous au vRealize Automation lien vers la matrice de support dans la [documentation du produit vRealize Automation](#).
- Consultez la *Matrice d'interopérabilité des produits VMware* sur le site Web VMware pour obtenir des informations sur la compatibilité avec d'autres produits VMware. Reportez-vous au vRealize Automation lien vers les matrices d'interopérabilité dans la [documentation du produit vRealize Automation](#).
- Vérifiez que l'instance de vRealize Automation que vous mettez à niveau se trouve dans une condition de fonctionnement stable. Corrigez tous les problèmes avant la mise à niveau.
- Assurez-vous d'avoir modifié les paramètres du délai d'expiration d'équilibrage de charge de la valeur par défaut à au moins 10 minutes.

Configuration matérielle requise

Vérifiez que le matériel de votre environnement est adapté à la version de vRealize Automation dans laquelle vous effectuez la mise à niveau.

Reportez-vous à [Spécifications matérielles et capacité maximale de vRealize Automation](#)

Vérifiez que les conditions préalables suivantes sont réunies avant de commencer une mise à niveau.

- Avant de procéder à la mise à niveau, vous devez au moins disposer de la configuration suivante : 18 Go de RAM, 4 CPU, Disque1 = 50 Go, Disque3 = 25 Go et Disque4 = 50 Go.

Si la machine virtuelle est sur vCloud Networking and Security, vous devrez éventuellement allouer plus d'espace RAM.

Bien que vCloud Networking and Security ne bénéficie plus du support technique, les propriétés personnalisées de VCNS restent valides pour NSX. Consultez l'[article 2144733 de la base de connaissances](#).

- Ces nœuds doivent disposer d'au moins 5 Go d'espace disque libre :
 - Site Web IaaS principal
 - Base de données Microsoft SQL
 - Model Manager
- Pour télécharger et exécuter la mise à niveau, vous devez disposer des ressources suivantes :
 - Au moins 15 Go sur la partition racine
 - 5 Go sur la partition `/storage/db` pour dispositif vRealize Automation master
 - 15 Go sur la partition racine pour chaque dispositif virtuel de réplica
- Vérifiez le sous-dossier `/storage/log` et supprimez les anciens fichiers ZIP archivés pour libérer de l'espace.

Conditions préalables générales

Vérifiez que les conditions préalables suivantes sont réunies avant de commencer une mise à niveau.

- Sauvegardez le fichier `setenv.sh` avant de démarrer la mise à niveau, car les mises à jour personnalisées de ce fichier sont remplacées après la mise à niveau. Le fichier se trouve dans `/usr/lib/vco/app-server/bin/setenv.sh`. Mettez à jour les valeurs au moment approprié après la mise à niveau et redémarrez `vco-server` pour appliquer les modifications.
- Vous avez accès à toutes les bases de données et à tous les équilibres de charge affectés par ou participant à la mise à niveau de vRealize Automation.
- Vous rendez le système indisponible pour les utilisateurs pendant que vous effectuez la mise à niveau.
- Vous désactivez les applications qui interrogent vRealize Automation.
- Vérifiez que le coordinateur de transaction distribué Microsoft (MS DTC) est activé sur tous les serveurs vRealize Automation et SQL associés. Pour des instructions, consultez [l'article 2089503 de la base de connaissances](#).
- Suivez ces étapes si vous mettez à niveau un environnement distribué configuré avec une base de données PostgreSQL intégrée.
 - a Examinez les fichiers dans le répertoire `pgdata` sur l'hôte master avant de mettre à niveau les hôtes de réplica.
 - b Accédez au dossier de données PostgreSQL sur l'hôte master dans `/var/vmware/vpostgres/current/pgdata/`.
 - c Fermez et supprimez tous les fichiers `.swp` dans le répertoire `pgdata`. Les fichiers portant le suffixe `.swp` vous obligent à fermer la session VI et à supprimer le fichier.

- d Vérifiez que tous les fichiers contenus dans ce répertoire ont le nom du propriétaire adéquat : postgres:<owner-group>.
- Si vous utilisez le plug-in DynamicTypes, exportez la configuration du plug-in DynamicTypes vRealize Orchestrator en tant que module.
 - a Connectez-vous à Java Client en tant qu'utilisateur administrateur.
 - b Sélectionnez l'onglet **Workflows**.
 - c Sélectionnez **Bibliothèque > Types dynamiques > Configuration**.
 - d Sélectionnez le workflow **Exporter la configuration en tant que module** et exécutez-le.
 - e Cliquez sur **Non définie > Insérer valeur**.
 - f Sélectionnez les espaces de nommage à exporter et cliquez sur **Ajouter** pour les ajouter au module.
 - g Cliquez sur **Envoyer** pour exporter le module.

En outre, vérifiez que les propriétés personnalisées ne comportent pas d'espaces dans leurs noms. Avant la mise à niveau vers cette version de vRealize Automation, supprimez tous les caractères d'espace de vos noms de propriétés personnalisées, par exemple remplacez l'espace par le caractère underscore, afin de permettre à la propriété personnalisée d'être reconnue dans l'installation mise à jour de vRealize Automation. Les noms des propriétés personnalisées vRealize Automation ne peuvent pas contenir d'espaces. Ce problème peut avoir une incidence sur l'utilisation d'une installation vRealize Orchestrator mise à niveau qui utilise des propriétés personnalisées qui contenaient des espaces dans les versions antérieures de vRealize Automation, de vRealize Orchestrator ou des deux.

Liste de contrôle pour la mise à niveau de vRealize Automation

Lorsque vous effectuez une mise à niveau depuis vRealize Automation 7.x ou version ultérieure, vous mettez à jour tous les composants vRealize Automation dans un ordre spécifique.

L'ordre de mise à niveau varie selon que vous effectuez la mise à niveau d'un environnement minimal ou d'un environnement distribué comprenant plusieurs dispositifs vRealize Automation.

Utilisez les listes de contrôle pour faire le suivi de votre travail pendant la mise à niveau. Effectuez les tâches dans l'ordre dans lequel elles sont fournies.




Tableau 1-45. Liste de contrôle pour la mise à niveau d'un environnement vRealize Automation minimal

Tâche	Instructions
<input type="checkbox"/> Exécutez une collecte de données d'inventaire de réseau et de sécurité de NSX avant de procéder à la mise à niveau. Cela est requis uniquement lorsque vRealize Automation est intégré à NSX.	Reportez-vous à Exécuter la collecte de données d'inventaire réseau et de sécurité NSX avant la mise à niveau de vRealize Automation .
<input type="checkbox"/> Sauvegardez votre installation actuelle. Cette étape est indispensable.	<p>Pour plus d'informations sur la sauvegarde et la restauration de votre système, reportez-vous à Sauvegarder votre environnement vRealize Automation existant.</p> <p>Pour obtenir des informations générales, reportez-vous au document <i>Configuring Backup and Restore by Using Symantec NetBackup</i> (Configuration de la sauvegarde et la restauration à l'aide de Symantec NetBackup) à l'adresse http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf</p>
<input type="checkbox"/> Téléchargez la mise à jour sur le dispositif vRealize Automation.	Reportez-vous à Téléchargement des mises à jour du dispositif vRealize Automation .
<input type="checkbox"/> Installez la mise à jour sur le dispositif vRealize Automation et les composants IaaS.	Reportez-vous à Installez la mise à jour sur le dispositif vRealize Automation et les composants IaaS .

Tableau 1-46. Liste de contrôle pour la mise à niveau d'un environnement vRealize Automation distribué

Tâche	Instructions
<input type="checkbox"/> Exécutez la collecte de données d'inventaire réseau et de sécurité NSX avant de mettre à niveau vRealize Automation 7.x. Cette intervention est requise uniquement lorsque vRealize Automation est intégré à NSX.	Reportez-vous à Exécuter la collecte de données d'inventaire réseau et de sécurité NSX avant la mise à niveau de vRealize Automation .
<input type="checkbox"/> Sauvegardez votre installation actuelle. Cette étape est indispensable.	<p>Pour plus d'informations sur la sauvegarde et la restauration de votre système, reportez-vous à Sauvegarder votre environnement vRealize Automation existant.</p> <p>Pour obtenir des informations détaillées, reportez-vous au document <i>Configuring Backup and Restore by Using Symantec NetBackup</i> (Configuration de la sauvegarde et la restauration à l'aide de Symantec NetBackup) à l'adresse http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf</p>
<input type="checkbox"/> Si vous mettez à niveau vRealize Automation 7.3.x, désactivez le basculement automatique de PostgreSQL.	Reportez-vous à Définissez le mode de réplication PostgreSQL vRealize Automation sur Asynchrone .
<input type="checkbox"/> Téléchargez les mises à jour sur le dispositif vRealize Automation.	Reportez-vous à Téléchargement des mises à jour du dispositif vRealize Automation .

Tableau 1-46. Liste de contrôle pour la mise à niveau d'un environnement vRealize Automation distribué (suite)

Tâche	Instructions
 Désactivez votre équilibrage de charge.	<p>Désactivez chaque nœud secondaire et supprimez les moniteurs de santé de vRealize Automation pour les éléments suivants.</p> <ul style="list-style-type: none"> ■ Dispositif vRealize Automation ■ Site Web IaaS ■ IaaS Manager Service <p>Pour une mise à niveau réussie, vérifiez les éléments suivants :</p> <ul style="list-style-type: none"> ■ Le trafic d'équilibrage de charge est uniquement dirigé vers le nœud principal. ■ Les moniteurs de santé vRealize Automation sont supprimés pour le dispositif, le site Web et Manager Service.
 Installez la mise à jour sur le dispositif vRealize Automation master et les composants IaaS.	Reportez-vous à Installez la mise à jour sur le dispositif vRealize Automation et les composants IaaS..
<p>Note Vous devez installer la mise à jour sur le dispositif master dans un environnement distribué.</p>	
 Activez votre équilibrage de charge.	Activer vos équilibres de charge

Interfaces utilisateur de l'environnement vRealize Automation

Utilisez et gérez votre environnement vRealize Automation avec plusieurs interfaces.

interfaces utilisateur

Ces tableaux décrivent les interfaces qui permettent de gérer votre environnement vRealize Automation.

Tableau 1-47. Console d'administration vRealize Automation

Objectif	Accès	Informations d'identification requises
Utilisez la console vRealize Automation pour ces tâches de l'administrateur système.	1 Démarrez un navigateur et ouvrez la page de démarrage du dispositif vRealize Automation en utilisant le nom de domaine complet du dispositif virtuel :	Vous devez être un utilisateur disposant du rôle administrateur système.
<ul style="list-style-type: none"> ■ Ajouter des locataires. ■ Personnaliser l'interface utilisateur vRealize Automation. ■ Configurer les serveurs de messagerie. ■ Afficher les journaux des événements. ■ Configurez vRealize Orchestrator. 	<p>https://vrealize-automation-appliance-FQDN.</p> <p>2 Cliquez sur vRealize Automation Console.</p> <p>Vous pouvez également utiliser cette URL pour ouvrir la console vRealize Automation :</p> <p>https://vrealize-automation-appliance-FQDN/vcac</p>	
	3 Connectez-vous.	

Tableau 1-48. Console de locataire vRealize Automation. Cette interface est l'interface utilisateur principale que vous utilisez pour créer et gérer vos services et ressources.

Objectif	Accès	Informations d'identification requises
<p>Utilisez vRealize Automation pour ces tâches.</p> <ul style="list-style-type: none"> ■ Demander de nouveaux Blueprints de service informatique. ■ Créer et gérer des ressources cloud et informatiques. ■ Créer et gérer des groupes personnalisés. ■ Créer et gérer des groupes d'activité. ■ Attribuer des rôles aux utilisateurs 	<ol style="list-style-type: none"> 1 Démarrez un navigateur et entrez l'URL de votre locataire en utilisant le nom de domaine complet du dispositif virtuel et le nom de l'URL du locataire : https://vrealize-automation-appliance-FQDN/vcac/org/tenant_URL_name . 2 Connectez-vous. 	<p>Vous devez être un utilisateur disposant d'un ou de plusieurs de ces rôles :</p> <ul style="list-style-type: none"> ■ Architecte d'application ■ Administrateur d'approbations ■ Administrateur du catalogue ■ Administrateur de conteneur ■ Architecte de conteneur ■ Consommateur de santé ■ Architecte d'infrastructure ■ Consommateur d'exportation sécurisée ■ Architecte de logiciel ■ Administrateur de locataire ■ Architecte XaaS

Tableau 1-49. Interface de gestion du dispositif vRealize Automation.

Objectif	Accès	Informations d'identification requises
<p>Utilisez la gestion des dispositifs vRealize Automation pour ces tâches.</p> <ul style="list-style-type: none"> ■ Afficher l'état des services enregistrés. ■ Afficher les informations système et redémarrer ou arrêter le dispositif. ■ Gérer la participation au Programme d'amélioration du produit. ■ Afficher l'état du réseau. ■ Afficher l'état de mise à jour et installer les mises à jour. ■ Gérer les paramètres d'administration. ■ Gérer les paramètres de l'hôte vRealize Automation. ■ Gérer les paramètres SSO. ■ Gérer les licences des produits. ■ Configurer la base de données Postgres vRealize Automation. ■ Configurer la messagerie vRealize Automation. ■ Configurer la journalisation vRealize Automation. ■ Installer les composants IaaS. ■ Migrer à partir d'une installation vRealize Automation existante ■ Gérer les certificats des composants IaaS ■ Configurer le service Xenon. 	<ol style="list-style-type: none"> 1 Démarrez un navigateur et ouvrez la page de démarrage du dispositif vRealize Automation en utilisant le nom de domaine complet du dispositif virtuel : <code>https://vrealize-automation-appliance-FQDN</code> 2 Cliquez sur Gestion de dispositifs vRealize Automation. Vous pouvez également utiliser cette URL pour ouvrir l'interface de gestion du dispositif vRealize Automation : <code>https://vrealize-automation-appliance-FQDN:5480</code> 3 Connectez-vous. 	<ul style="list-style-type: none"> ■ Nom d'utilisateur : root ■ Mot de passe : mot de passe que vous avez entré lorsque vous avez déployé le dispositif vRealize Automation.

Tableau 1-50. Client vRealize Orchestrator

Objectif	Accès	Informations d'identification requises
<p>Utilisez le client vRealize Orchestrator pour effectuer ces tâches.</p> <ul style="list-style-type: none"> ■ Développer des actions. ■ Développer des workflows. ■ Gérer des stratégies. ■ Installer des modules. ■ Gérer les autorisations d'utilisateur et de groupe d'utilisateurs. ■ Attacher des balises à des objets URI. ■ Afficher l'inventaire. 	<ol style="list-style-type: none"> 1 Démarrez un navigateur et ouvrez la page de démarrage vRealize Automation en utilisant le nom de domaine complet du dispositif virtuel : https://vrealize-automation-appliance-FQDN 2 Pour télécharger le fichier client.jnlp sur votre ordinateur local, cliquez sur vRealize Orchestrator Client. 3 Cliquez avec le bouton droit de la souris sur le fichier client.jnlp et sélectionnez Lancer. 4 Dans la boîte de dialogue Voulez-vous continuer ?, cliquez sur Continuer. 5 Connectez-vous. 	<p>Vous devez être un utilisateur disposant du rôle d'administrateur système ou appartenir au groupe vcoadmins configuré dans les paramètres de fournisseur d'authentification du centre de contrôle vRealize Orchestrator.</p>

Tableau 1-51. Centre de contrôle vRealize Orchestrator

Objectif	Accès	Informations d'identification requises
<p>Utilisez le centre de contrôle vRealize Orchestrator pour modifier la configuration de l'instance par défaut de vRealize Orchestrator qui est intégrée dans vRealize Automation.</p>	<ol style="list-style-type: none"> 1 Démarrez un navigateur et ouvrez la page de démarrage du dispositif vRealize Automation en utilisant le nom de domaine complet du dispositif virtuel : https://vrealize-automation-appliance-FQDN 2 Cliquez sur Gestion de dispositifs vRealize Automation. Vous pouvez également utiliser cette URL pour ouvrir l'interface de gestion du dispositif vRealize Automation : https://vrealize-automation-appliance-FQDN:5480 3 Connectez-vous. 4 Cliquez sur vRA > Orchestrator. 5 Sélectionnez l'interface utilisateur d'Orchestrator. 6 Cliquez sur Démarrer. 7 Cliquez sur l'URL de l'interface utilisateur d'Orchestrator. 8 Connectez-vous. 	<p>Nom d'utilisateur</p> <ul style="list-style-type: none"> ■ Entrez root si l'authentification basée sur les rôles n'est pas configurée. ■ Entrez votre nom d'utilisateur vRealize Automation s'il est configuré pour l'authentification basée sur les rôles. <p>Mot de passe</p> <ul style="list-style-type: none"> ■ Entrez le mot de passe que vous avez entré lorsque vous avez déployé le dispositif vRealize Automation si l'authentification basée sur les rôles n'est pas configurée. ■ Entrez le mot de passe de votre nom d'utilisateur si ce dernier est configuré pour l'authentification basée sur les rôles.

Tableau 1-52. Invite de commande Linux

Objectif	Accès	Informations d'identification requises
Utilisez l'invite de commande Linux sur un hôte, tels que l'hôte du dispositif vRealize Automation, pour ces tâches. <ul style="list-style-type: none"> ■ Arrêter ou démarrer les services ■ Modifier les fichiers de configuration ■ Exécuter des commandes ■ Récupérer des données 	<ol style="list-style-type: none"> 1 Sur l'hôte du dispositif vRealize Automation, ouvrez une nouvelle invite de commande. Pour ouvrir l'invite de commande sur votre ordinateur local, vous pouvez démarrer une session sur l'hôte à l'aide d'une application telle que PuTTY. 2 Connectez-vous. 	<ul style="list-style-type: none"> ■ Nom d'utilisateur : root ■ Mot de passe : mot de passe que vous avez créé lorsque vous avez déployé le dispositif vRealize Automation.

Tableau 1-53. Invite de commande Windows

Objectif	Accès	Informations d'identification requises
Vous pouvez utiliser une invite de commande Windows sur un hôte, tel que l'hôte IaaS, pour exécuter des scripts.	<ol style="list-style-type: none"> 1 Sur l'hôte IaaS, connectez-vous à Windows. Pour vous connecter à partir de votre ordinateur local, vous pouvez démarrer une session de poste de travail distante. 2 Ouvrez l'invite de commande Windows. Pour ouvrir l'invite de commande, cliquez avec le bouton droit sur l'icône Démarrer sur l'hôte et sélectionnez Invite de commande ou Invite de commande (admin). 	<ul style="list-style-type: none"> ■ Nom d'utilisateur : utilisateur disposant de privilèges administratifs. ■ Mot de passe : mot de passe de l'utilisateur.

Mise à niveau de produits VMware intégrés à vRealize Automation

Vous devez gérer tous les produits VMware intégrés à votre environnement vRealize Automation lorsque vous procédez à la mise à niveau de vRealize Automation.

Si votre environnement vRealize Automation est intégré à un ou plusieurs autres produits, vous devez mettre à niveau vRealize Automation avant de mettre à jour les autres produits. Si vRealize Business for Cloud est intégré à vRealize Automation, vous devez annuler l'enregistrement de vRealize Business for Cloud avant de mettre à niveau vRealize Automation.

Suivez le workflow suggéré pour gérer les produits intégrés lorsque vous procédez à la mise à niveau de vRealize Automation.

- 1 Mettez à niveau vRealize Automation.
- 2 Mettez à niveau VMwarevRealize Operations Manager.
- 3 Mettez à niveau VMwarevRealize Log Insight.
- 4 Mettez à niveau VMwarevRealize Business for Cloud.

Cette section fournit des conseils supplémentaires sur la gestion de vRealize Business for Cloud lorsqu'il est intégré à votre environnement vRealize Automation.

Mise à niveau de vRealize Operations Manager intégré à vRealize Automation

Procédez à la mise à niveau de vRealize Operations Manager après avoir mis à niveau vRealize Automation.

Procédure

- 1 Mettez à niveau vRealize Automation.
- 2 Mettez à niveau vRealize Operations Manager. Pour plus d'informations, reportez-vous à la section *Mise à niveau de votre logiciel* dans la documentation de [VMware vRealize Operations Manager](#).

Mise à niveau de vRealize Log Insight intégré à vRealize Automation

Procédez à la mise à niveau de vRealize Log Insight après avoir mis à niveau vRealize Automation.

Procédure

- 1 Mettez à niveau vRealize Automation.
- 2 Mettez à niveau vRealize Log Insight. Pour plus d'informations, reportez-vous à la section *Mise à niveau de vRealize Log Insight* dans la documentation de [VMware vRealize Log Insight](#).

Mise à niveau de vRealize Business for Cloud intégré à vRealize Automation

Lorsque vous mettez à niveau votre environnement vRealize Automation, vous devez annuler l'enregistrement de votre connexion à vRealize Business for Cloud, puis enregistrer à nouveau la connexion.

Effectuez cette procédure pour garantir la continuité du service avec vRealize Business for Cloud lorsque vous mettez à niveau votre environnement vRealize Automation.

Procédure

- 1 Annulez l'enregistrement de vRealize Business for Cloud depuis vRealize Automation. Reportez-vous à la section *Annuler l'enregistrement de vRealize Business for Cloud depuis vRealize Automation* dans la documentation de [VMware vRealize Business for Cloud](#).
- 2 Mettez à niveau vRealize Automation.
- 3 Si nécessaire, mettez à niveau vRealize Business for Cloud. Reportez-vous à la section *Mise à niveau de vRealize Business for Cloud* dans la documentation de [VMware vRealize Business for Cloud](#).
- 4 Enregistrez vRealize Business for Cloud dans vRealize Automation. Reportez-vous à la section *Enregistrer vRealize Business for Cloud avec vRealize Automation* dans la documentation de [VMware vRealize Business for Cloud](#).

Préparation de la mise à niveau de vRealize Automation

Effectuez les tâches suivantes avant de procéder à la mise à niveau de vRealize Automation 7.x.

Effectuez les tâches dans l'ordre indiqué dans la liste de contrôle. Reportez-vous à [Liste de contrôle pour la mise à niveau de vRealize Automation](#).

Exécuter la collecte de données d'inventaire réseau et de sécurité NSX avant la mise à niveau de vRealize Automation

Avant la mise à niveau de vRealize Automation 7.1 ou version ultérieure, vous devez exécuter la collecte de données d'inventaire réseau et de sécurité NSX dans l'environnement source vRealize Automation 7.1 ou version ultérieure à partir duquel vous effectuez la mise à niveau.

Cette collecte de données est nécessaire pour que l'action de reconfiguration de l'équilibrage de charge fonctionne dans vRealize Automation pour les déploiements.

Procédure

- ◆ Exécutez la collecte de données d'inventaire réseau et de sécurité NSX dans l'environnement source vRealize Automation 7.1 ou version ultérieure à partir duquel vous effectuez la mise à niveau. Reportez-vous à [Démarrer la collecte de données de point de terminaison manuellement](#).

Étape suivante

[Conditions préalables de sauvegarde pour la mise à niveau de vRealize Automation](#).

Conditions préalables de sauvegarde pour la mise à niveau de vRealize Automation

Réunissez les conditions préalables à la sauvegarde avant de commencer la mise à niveau.

Conditions préalables

- Vérifiez que l'environnement source est entièrement installé et configuré.
- Connectez-vous à votre client vSphere et, pour chaque dispositif dans votre environnement source, sauvegardez tous les fichiers de configuration du dispositif vRealize Automation dans les répertoires suivants :
 - /etc/vcac/
 - /etc/vco/
 - /etc/apache2/
 - /etc/rabbitmq/
- Sauvegardez la base de données Microsoft SQL Server d'IaaS. Pour plus d'informations, recherchez des articles sur le [Réseau des développeurs Microsoft](#) concernant la création d'une sauvegarde complète de la base de données SQL Server.
- Sauvegardez tous les fichiers que vous avez personnalisés, par exemple DataCenterLocations.xml.

- Créez un snapshot de chaque dispositif virtuel et de chaque serveur IaaS. Suivez les directives standard relatives à la sauvegarde de l'ensemble du système en cas d'échec de la mise à niveau de vRealize Automation. Reportez-vous à [Sauvegarde et récupération des installations de vRealize Automation](#).

Sauvegarder votre environnement vRealize Automation existant

Si la mise à jour échoue, utilisez le snapshot pour revenir à la dernière configuration correcte connue et tentez une nouvelle mise à niveau.

Conditions préalables

Avant de procéder à la mise à niveau de vRealize Automation 7.1 ou version ultérieure, arrêtez le système et prenez un snapshot de chaque serveur IaaS vRealize Automation sur chaque nœud Windows et de chaque dispositif vRealize Automation sur chaque nœud Linux.

- [Conditions préalables de sauvegarde pour la mise à niveau de vRealize Automation](#).
- La base de données PostgreSQL est configurée en mode haute disponibilité. Connectez-vous à l'interface de gestion des dispositifs vRealize Automation et sélectionnez **Cluster** pour rechercher le nœud master actuel. Si la configuration de la base de données est répertoriée comme une base de données externe, créez une sauvegarde manuelle de cette base de données externe.
- Si la base de données Microsoft SQL de vRealize Automation n'est pas hébergée sur le serveur IaaS, créez un fichier de sauvegarde de base de données.
- Vérifiez que vous remplissez les conditions requises de sauvegarde pour la mise à niveau.
- Vérifiez que vous avez créé un snapshot de votre système pendant qu'il est à l'arrêt. C'est la méthode préférée de prise d'un snapshot. Pour plus d'informations sur la création et la gestion de snapshots, reportez-vous à la [documentation du produit vSphere](#).

Note Lorsque vous sauvegardez le dispositif vRealize Automation et les composants IaaS, désactivez les snapshots en mémoire et les snapshots mis au repos.

- Si vous avez modifié l'un des fichiers *.exe.config (par exemple, managervice.exe.config) sur vos serveurs IaaS, effectuez une sauvegarde de ce fichier. Reportez-vous à [Restaurer les modifications apportées à la connexion dans le fichier app.config](#).
- Sauvegardez les fichiers de configuration du workflow externe (xmldb). Reportez-vous à [Restaurer les fichiers de délai d'expiration du workflow externe](#).
- Vérifiez que vous disposez d'un emplacement à l'extérieur de votre dossier actuel dans lequel vous pouvez stocker votre fichier de sauvegarde. Reportez-vous à [Copies de sauvegarde de fichiers .xml entraînant l'expiration du délai du système](#).

Procédure

- 1 Connectez-vous à votre client vSphere.

- 2 Localisez chaque machine vRealize Automation IaaS Windows, et chaque nœud de dispositif vRealize Automation.
- 3 Pour préserver l'intégrité des données, vous devez arrêter dans un ordre spécifique. Si vous utilisez vCenter Server pour gérer vos machines virtuelles, utilisez la commande `shutdown` invitée pour arrêter vRealize Automation. Reportez-vous à [Arrêter vRealize Automation](#) et suivez l'ordre indiqué.
- 4 Prenez un snapshot de chaque machine vRealize Automation.
- 5 Utilisez votre méthode de sauvegarde préférée pour créer une sauvegarde complète de chaque nœud de dispositif.
- 6 Lorsque vous démarrez vRealize Automation à partir du début, par exemple après une coupure de courant, une mise à l'arrêt ou une récupération, vous devez démarrer les composants dans un ordre spécifique. Pour plus d'informations, reportez-vous à [Démarrer vRealize Automation](#).
- 7 Connectez-vous à chaque console de gestion de dispositif vRealize Automation et vérifiez que le système est entièrement opérationnel.
 - a Cliquez sur **Services**.
 - b Vérifiez que chaque service est ENREGISTRÉ.

Étape suivante

[Définissez le mode de réplication PostgreSQL vRealize Automation sur Asynchrone.](#)

Définissez le mode de réplication PostgreSQL vRealize Automation sur Asynchrone

Si vous procédez à la mise à niveau à partir d'un environnement distribué vRealize Automation qui fonctionne en mode de réplication synchrone PostgreSQL, vous devez le modifier en mode asynchrone avant d'effectuer la mise à niveau.

Conditions préalables

Vous avez un environnement distribué vRealize Automation que vous souhaitez mettre à niveau.

Procédure

- 1 Connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Cliquez sur **Cluster**.
- 3 Cliquez sur **Mode asynchrone** et attendez la fin de l'action.
- 4 Vérifiez que tous les nœuds dans la colonne État de synchronisation affichent l'état Asynchrone.

Étape suivante

Téléchargement des mises à jour du dispositif vRealize Automation

Téléchargement des mises à jour du dispositif vRealize Automation

Vous pouvez rechercher les mises à jour à partir de l'interface de gestion du dispositif vRealize Automation et les télécharger en utilisant l'une des méthodes suivantes.

Pour garantir les meilleures performances de mise à niveau, utilisez la méthode de fichier ISO. Pour obtenir des performances de mise à niveau optimales ou si l'accès à Internet pour télécharger des fichiers RPM est limité, utilisez la méthode de fichier ISO pour extraire localement update_repo.iso dans votre banque de données.

Pour éviter les problèmes potentiels lors de la mise à niveau de votre dispositif, ou si des problèmes surgissent pendant la mise à niveau du dispositif, reportez-vous à [l'article de la base de connaissances VMware](#) *La mise à niveau de vRealize Automation échoue en raison des doublons dans la base de données de vRealize Orchestrator (54987)*.

Télécharger les mises à jour de dispositif virtuel pour une utilisation avec un lecteur de CD-ROM

Vous pouvez mettre à jour votre dispositif virtuel à partir d'un fichier ISO que le dispositif lit à partir du lecteur de CD-ROM virtuel. C'est la méthode préférée.

Vous téléchargez le fichier ISO et configurez le dispositif principal afin d'utiliser ce fichier pour mettre à niveau votre dispositif.

Conditions préalables

- Sauvegardez votre environnement vRealize Automation existant.
- Vérifiez que tous les lecteurs de CD-ROM utilisés dans votre mise à niveau sont activés avant de procéder à la mise à jour d'un dispositif vRealize Automation. Reportez-vous à la documentation de vSphere pour obtenir des informations sur l'ajout d'un lecteur de CD-ROM à une machine virtuelle dans le client vSphere.

Procédure

- 1 Téléchargez le fichier ISO du référentiel de mise à jour.
 - a Démarrez un navigateur et accédez à la [page du produit vRealize Automation](#) à l'adresse www.vmware.com.
 - b Cliquez sur **Ressources de téléchargement de vRealize Automation** pour accéder à la page de téléchargement de VMware.
 - c Téléchargez le fichier approprié.
- 2 Localisez le fichier téléchargé sur votre système pour vérifier que la taille du fichier est la même que celle du fichier de la page de téléchargement VMware. Utilisez les totaux de contrôle fournis sur la page de téléchargement pour valider l'intégrité du fichier téléchargé. Pour plus d'informations, reportez-vous aux liens figurant en bas de la page de téléchargement VMware.
- 3 Vérifiez que votre dispositif virtuel principal est sous tension.

- 4 Connectez le lecteur de CD-ROM du dispositif virtuel principal au fichier ISO que vous avez téléchargé.

Note Connectez-vous au dispositif et montez le CD-ROM dans Linux à l'aide de ce chemin de fichier `mount/dev/sr0/media/cdrom` si vous ne pouvez pas voir la mise à jour une fois que le fichier ISO est attaché à la machine virtuelle.

- 5 Sur votre dispositif vRealize Automation principal, connectez-vous à la gestion des dispositifs vRealize Automation en tant qu'utilisateur **racine** à l'aide du mot de passe que vous avez entré lorsque vous avez déployé le dispositif vRealize Automation.
- 6 Cliquez sur l'onglet **Mettre à jour**.
- 7 Cliquez sur **Paramètres**.
- 8 Sous Référentiel de mises à jour, sélectionnez **Utiliser les mises à jour de CD-ROM**.
- 9 Cliquez sur **Enregistrer les paramètres**.

Télécharger les mises à jour du dispositif vRealize Automation dans un référentiel VMware
Vous pouvez télécharger la mise à jour de votre dispositif vRealize Automation à partir d'un référentiel public sur le site Web vmware.com.

Conditions préalables

- Sauvegardez votre environnement vRealize Automation existant.
- Vérifiez que votre dispositif vRealize Automation est sous tension.

Procédure

- 1 Sur votre dispositif vRealize Automation principal, connectez-vous à la gestion des dispositifs vRealize Automation en tant qu'utilisateur **racine** à l'aide du mot de passe que vous avez entré lorsque vous avez déployé le dispositif vRealize Automation.
- 2 Cliquez sur l'onglet **Mettre à jour**.
- 3 Cliquez sur **Paramètres**.
- 4 (Facultatif) Définissez la fréquence de vérification des mises à jour dans le volet Mises à jour automatiques.
- 5 Dans le volet Référentiel de mises à jour, sélectionnez **Utiliser le référentiel par défaut**.
Le référentiel par défaut est défini sur l'URL correcte VMware.com.
- 6 Cliquez sur **Enregistrer les paramètres**.

Nettoyage de la base de données Postgres

Pour préparer votre base de données postgres pour la mise à niveau ou la migration, effectuez un nettoyage de la base de données.

Les objets volumineux du tableau pg_largeobject, qui stockent les bundles de journaux et de télémétrie, ainsi que les objets d'application, peuvent ralentir ou arrêter votre mise à niveau ou votre migration. Avant de tenter de mettre à niveau ou de migrer, vous pouvez préparer votre base de données postgres en effectuant un nettoyage de base de données à vide.

Note Le nettoyage de la base de données ne peut pas être effectué lorsque des services sont en cours d'exécution.

Procédure

- 1 Commencez par sauvegarder votre dispositif en créant un vidage de base de données postgres à partir de la page Cluster dans l'interface VAMI ou en effectuant ou sauvegardant un snapshot du dispositif virtuel master.

- 2 À partir de l'interface VAMI vRA, basculez la réplication de synchrone vers asynchrone.

- 3 En tant qu'utilisateur postgres sur le vRA master (su - postgres), videz la base de données pour supprimer les entrées du journal.

```
su - postgres -c "/opt/vmware/vpostgres/current/bin/vacuumlo -v -p 5432 vcac"
```

```
su - postgres -c "/opt/vmware/vpostgres/current/bin/vacuumdb -f -p 5432 -t pg_largeobject  
-t pg_largeobject_metadata vcac"
```

- 4 Pour récupérer de l'espace de base de données, utilisez les commandes de vidage complet.

```
psql -d vcac
```

```
vacuum full
```

```
vacuum analyze
```

Mise à jour du dispositif vRealize Automation et des composants IaaS

Après avoir réuni les conditions préalables à la mise à niveau et après avoir téléchargé la mise à jour du dispositif virtuel, installez la mise à jour.

Pour un environnement minimal, vous installez la mise à jour sur le dispositif vRealize Automation. Pour un environnement distribué, installez la mise à jour sur le nœud de dispositif master. Le temps requis pour terminer la mise à jour dépend de votre environnement et de votre réseau. Une fois la mise à jour terminée, le système affiche les modifications apportées à la page État de la mise à jour de la gestion de dispositifs vRealize Automation. Une fois la mise à jour du dispositif terminée, redémarrez le dispositif. Lorsque vous redémarrez le dispositif master dans un environnement distribué, le système redémarre chaque nœud de réplica.

Après le redémarrage, En attente du démarrage des services VA s'affiche sur la page État de la mise à jour. La mise à jour d'IaaS démarre lorsque le système est entièrement initialisé et que tous les services sont en cours d'exécution. Vous pouvez observer la progression de la mise à niveau d'IaaS sur la page État de la mise à jour. Le premier composant du serveur IaaS peut prendre environ 30 minutes. Pendant la mise à niveau, un message similaire à Mise à niveau des composants de serveur du nœud web1-vra.mycompany.com.

À la fin du processus de mise à niveau de chaque nœud de Manager Service, vous voyez un message similaire à **Activation du mode de basculement automatique ManagerService** pour le nœud `mgr-vra.mycompany.com`. À partir de vRealize Automation 7.3, le nœud Manager Service actif passe d'une sélection manuelle à une décision système déterminant quel nœud devient le serveur de basculement. Le système permet l'exécution de cette fonctionnalité au cours de la mise à niveau. Si vous rencontrez des problèmes avec cette fonctionnalité, reportez-vous à la section [La mise à jour ne réussit pas à mettre à jour l'agent de gestion](#).

Installez la mise à jour sur le dispositif vRealize Automation et les composants IaaS.

Vous installez la mise à jour sur le dispositif virtuel vRealize Automation source pour mettre à niveau vRealize Automation et les composants IaaS vers la version vRealize Automation cible.

Ne fermez pas l'interface de gestion du dispositif vRealize Automation pendant que vous installez la mise à jour.

Si vous rencontrez des problèmes pendant le processus de mise à niveau, reportez-vous à [Résolution des problèmes de mise à niveau de vRealize Automation](#).

Note Lors d'une mise à niveau de l'agent de gestion sur les machines virtuelles IaaS, un certificat public VMware est temporairement installé dans votre magasin de certificats des éditeurs approuvés. Le processus de mise à niveau de l'agent de gestion utilise un script PowerShell qui est signé avec ce certificat. Lorsque la mise à niveau est terminée, ce certificat est supprimé de votre magasin de certificats.

Conditions préalables

- Vérifiez que vous avez sélectionné une méthode de téléchargement et terminé la procédure de cette méthode. Reportez-vous à [Téléchargement des mises à jour du dispositif vRealize Automation](#).
- Pour tous les environnements haute disponibilité, reportez-vous à [Sauvegarder votre environnement vRealize Automation existant](#).
- Pour les environnements disposant d'équilibrages de charge, vérifiez que vous avez désactivé tous les nœuds redondants et supprimé les moniteurs de santé. Pour plus d'informations, consultez la documentation de votre équilibrage de charge.
 - Dispositif vRealize Automation
 - Site Web IaaS

■ IaaS Manager Service

Note Lors de l'exécution d'une mise à niveau automatique de vRealize Automation 7.4 ou version ultérieure, vous n'avez pas besoin de désactiver les moniteurs d'équilibrage de charge IaaS Web secondaires. Ne désactivez pas les moniteurs d'équilibrage de charge d'IaaS Manager Server avant la mise à niveau. Si vous mettez à niveau des nœuds IaaS manuellement à l'aide du programme d'installation d'IaaS hérité, vous devez désactiver le trafic pour les nœuds Web secondaires avant la mise à niveau.

- Pour les déploiements disposant d'équilibrages de charge, vérifiez que le trafic est uniquement dirigé vers le nœud principal.
- Pour vérifier que le service IaaS hébergé dans Microsoft Internet Information Services (IIS) s'exécute, procédez comme suit :
 - a Démarrez un navigateur et entrez l'URL
`https://webhostname/Repository/Data/MetaModel.svc` pour vérifier que le référentiel Web est en cours d'exécution. S'il fonctionne correctement, aucune erreur n'est retournée et une liste des modèles au format XML s'affiche.
 - b Connectez-vous au site Web IaaS et vérifiez que l'état enregistré dans le fichier `Repository.log` indique OK. Le fichier se trouve dans le dossier de base VCAC dans `/Server/Model Manager Web/Logs/Repository.log`.

Note Pour un site Web IaaS distribué, connectez-vous au site Web secondaire, sans MMD, puis arrêtez temporairement Microsoft IIS. Pour vous assurer que le trafic d'équilibrage de charge transite uniquement par le nœud Web principal, sélectionnez la connectivité `MetaModel.svc`, puis redémarrez Microsoft IIS.

- Pour vérifier que tous les nœuds IaaS sont dans un état sain, procédez comme suit :
 - a Connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.
`https://vrealize-automation-appliance-FQDN:5480`
 - b Sélectionnez **Cluster**.
 - c Sous **Dernière connexion**, vérifiez ce qui suit.
 - L'heure de la dernière connexion des nœuds IaaS dans le tableau remonte à moins de 30 secondes.
 - L'heure de la dernière connexion des nœuds du dispositif virtuel remonte à moins de 10 minutes.

Si les nœuds IaaS ne communiquent pas avec le dispositif vRealize Automation, la mise à niveau échoue.

Pour diagnostiquer les problèmes de connectivité entre l'agent de gestion et le dispositif virtuel, procédez comme suit.

- 1 Connectez-vous à chaque nœud IaaS qui n'est pas répertorié ou dont l'heure de **Dernière connexion** remonte à plus de 30 secondes.
 - 2 Consultez les journaux de l'agent de gestion pour voir si des erreurs sont enregistrées.
 - 3 Si l'agent de gestion n'est pas en cours d'exécution, redémarrez-le dans la console des services.
- d Notez d'éventuels nœuds orphelins répertoriés dans le tableau. Un nœud orphelin est un nœud dupliqué qui est signalé sur l'hôte mais n'y existe pas. Vous devez supprimer les nœuds orphelins. Pour plus d'informations, reportez-vous à [Supprimer les nœuds orphelins sur vRealize Automation](#).
- Si vous avez un dispositif virtuel de réplica qui ne fait plus partie du cluster, vous devez le supprimer du tableau du cluster. Si vous ne supprimez pas ce dispositif, le processus de mise à niveau affiche un message d'avertissement indiquant que la mise à jour du réplica a échoué.
 - Vérifiez que toutes les demandes enregistrées et en cours sont terminées avec succès avant de procéder à la mise à niveau.
 - Si vous mettez à niveau les composants IaaS manuellement après avoir mis à jour le dispositif vRealize Automation source, reportez-vous à la section [Exclure la mise à niveau d'IaaS](#). Si vous prévoyez de mettre à niveau IaaS manuellement, vous devez également arrêter tous les services IaaS, à l'exception de l'agent de gestion, sur chaque nœud IaaS.

Procédure

- 1 Connectez-vous à l'interface de gestion du dispositif principal ou master vRealize Automation en tant qu'utilisateur racine.

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

- 2 Cliquez sur **Services** et vérifiez que tous les services sont enregistrés.
- 3 Sélectionnez **Cluster** et vérifiez que le dispositif correspond au dispositif master vRealize Automation.

Vous installez la mise à jour uniquement sur le dispositif vRealize Automation master. Chaque dispositif vRealize Automation de réplica est mis à jour avec le dispositif master.

- 4 Sélectionnez **Mettre à jour > État**.
- 5 Cliquez sur **Vérifier les mises à jour** pour vérifier qu'une mise à jour est accessible.
- 6 (Facultatif) Pour des instances du dispositif vRealize Automation, cliquez sur **Détails** dans la zone Version du dispositif pour afficher les informations sur l'emplacement des notes de mise à jour.
- 7 Cliquez sur **Installer les mises à jour**.

8 Cliquez sur **OK**.

Un message indiquant que la mise à jour est en cours s'affiche. Le système affiche les modifications apportées pendant une mise à niveau sur la page de résumé de la mise à jour. Le temps requis pour terminer la mise à jour dépend de votre environnement et de votre réseau.

9 (Facultatif) Pour surveiller la mise à jour plus en détail, utilisez un émulateur de terminal pour vous connecter au dispositif principal. Affichez le fichier `updatecli.log` à l'emplacement `/opt/vmware/var/log/vami/updatecli.log`.

Des informations d'avancement de mise à niveau supplémentaires peuvent également être consultées dans ces fichiers.

- `/opt/vmware/var/log/vami/vami.log`
- `/var/log/vmware/horizon/horizon.log`
- `/var/log/bootstrap/*.log`

Si vous vous déconnectez pendant le processus de mise à niveau, vous pouvez continuer à suivre la progression de la mise à jour dans le fichier journal. Le fichier `updatecli.log` peut afficher des informations sur la version de vRealize Automation à partir de laquelle vous effectuez la mise à niveau. Cette version affichée devient la version appropriée plus tard pendant le processus de mise à niveau.

10 Lorsque la mise à jour du dispositif vRealize Automation est terminée, cliquez sur **Système > Redémarrer** dans l'interface de gestion du dispositif vRealize Automation.

Dans un environnement distribué, tous les nœuds de dispositif de réplica mis à niveau redémarrent lorsque vous redémarrez le dispositif master.

La mise à jour d'IaaS démarre lorsque le système est initialisé et que tous les services sont en cours d'exécution. Cliquez sur **Mise à jour > État** pour observer la progression de la mise à niveau d'IaaS.

11 Lorsque la mise à jour d'IaaS est terminée, cliquez sur **Cluster** dans l'interface de gestion du dispositif vRealize Automation et vérifiez que le numéro de version correspond à la version actuelle pour tous les nœuds et composants IaaS.**12** Cliquez sur **Télémétrie** dans l'interface de gestion du dispositif vRealize Automation. Lisez la remarque relative à la participation au programme d'amélioration du produit et choisissez de rejoindre ou non le programme.

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>.

Pour plus d'informations sur le Programme d'amélioration du produit, reportez-vous à la section [Rejoindre ou quitter le Programme d'amélioration du produit pour vRealize Automation](#).

Étape suivante

Si votre déploiement utilise un équilibrage de charge, procédez comme suit.

- 1 Activez les contrôles de santé de l'équilibrage de charge de vRealize Automation.
- 2 Réactivez le trafic d'équilibrage de charge pour tous les nœuds vRealize Automation.

Si la mise à niveau des composants IaaS échoue, reportez-vous à la section [Mise à niveau séparée des composants du serveur IaaS si le processus de mise à jour échoue](#)

Mise à niveau séparée des composants du serveur IaaS si le processus de mise à jour échoue

Si le processus de mise à jour automatique échoue, vous pouvez mettre à niveau les composants IaaS séparément.

Si le site Web vRealize Automation IaaS et Manager Service ont été mis à niveau, vous pouvez réexécuter le script shell de mise à niveau sans revenir aux snapshots que vous avez pris avant la mise à niveau. Parfois, un événement de redémarrage en attente généré lors de la mise à niveau de plusieurs composants IaaS installés sur la même machine virtuelle peut faire échouer la mise à niveau. Dans ce cas, essayez de redémarrer manuellement le nœud IaaS et de réexécuter la mise à niveau pour corriger le problème. Si la mise à niveau échoue toujours, contactez le support VMware ou tentez une mise à niveau manuelle en procédant comme suit.

- 1 Ramenez votre dispositif vRealize Automation à l'état qui était le sien avant la mise à jour.
- 2 Exécutez une commande pour exclure les composants IaaS du processus de mise à jour. Reportez-vous à [Exclure la mise à niveau d'IaaS](#).
- 3 Exécutez le processus de mise à jour sur le dispositif vRealize Automation.
- 4 Mettez à jour les composants IaaS séparément à l'aide du script shell de mise à niveau ou de la dernière version du module MSI du programme d'installation d'IaaS vRealize Automation.

Mettre à niveau les composants IaaS à l'aide du script shell de mise à niveau après la mise à niveau du dispositif vRealize Automation

Utilisez le script shell de mise à niveau pour mettre à niveau les composants IaaS après la mise à jour de chaque dispositif vRealize Automation 7.1 ou version ultérieure vers la version de vRealize Automation cible.

Le dispositif vRealize Automation mis à jour contient un script shell que vous utilisez pour mettre à niveau chaque nœud et composant IaaS.

Vous pouvez exécuter le script de mise à niveau à l'aide de la console vSphere pour la machine virtuelle ou à l'aide d'une session de console SSH. Si vous utilisez la console vSphere, vous évitez les problèmes de connectivité réseau intermittents qui peuvent interrompre l'exécution du script.

Si vous arrêtez le script pendant qu'il met à niveau un composant, le script s'arrête lorsqu'il a terminé cette mise à niveau. Si d'autres composants sur le nœud ont toujours besoin d'être mis à niveau, vous pouvez réexécuter le script.

Lorsque la mise à niveau est terminée, vous pouvez en vérifier le résultat en ouvrant le fichier journal de mise à niveau à l'emplacement `/opt/vmware/var/log/vami/upgrade-iaas.log`.

Conditions préalables

- Consultez [Résolution des problèmes de mise à niveau de vRealize Automation](#).
- Vérifiez l'aboutissement de la mise à niveau de tous les dispositifs vRealize Automation.
- Si vous redémarrez un serveur IaaS après avoir mis à jour tous les dispositifs vRealize Automation, mais avant la mise à niveau des composants IaaS, arrêtez tous les services Windows IaaS, sauf le service Agent de gestion.
- Avant d'exécuter le script shell de mise à niveau sur le nœud du dispositif vRealize Automation master, cliquez sur **Services** dans l'interface de gestion du dispositif vRealize Automation. Vérifiez que tous les services, sauf `iaas-service`, sont ENREGISTRÉS.
- Pour installer manuellement l'agent de gestion IaaS sur chaque nœud IaaS, respectez les étapes suivantes.
 - a Dans un navigateur, ouvrez la page d'installation d'IaaS sur le dispositif.
`https://vrealize-automation-appliance-FQDN:5480/installer`
 - b Téléchargez le programme d'installation de l'agent de gestion, `vCAC-iaasManagementAgent-Setup.msi`.
 - c Connectez-vous à chaque machine vRealize Automation IaaS et mettez à niveau l'agent de gestion avec le programme d'installation de l'agent de gestion. Redémarrez le service de l'agent de gestion Windows.
- Vérifiez que l'environnement d'exécution Java SE 8, 64 bits, Update 181 ou version ultérieure est installé sur votre nœud du site Web IaaS principal et de Model Manager. Après avoir installé Java, vous devez configurer la variable d'environnement `JAVA_HOME` sur la nouvelle version pour chaque nœud du serveur.
- Connectez-vous à chaque nœud de site Web IaaS et vérifiez que la date de création est antérieure à la date de modification dans le fichier `web.config`. Si la date de création du fichier `web.config` est identique ou ultérieure à la date de modification, suivez la procédure décrite dans [Échec de la mise à niveau pour le composant de site Web IaaS](#).
- Pour vérifier que chaque nœud IaaS a un agent de gestion IaaS mis à niveau, appliquez la procédure suivante à chaque nœud IaaS :
 - a Connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.
`https://vrealize-automation-appliance-FQDN:5480`
 - b Sélectionnez **Cluster**.
 - c Développez la liste de tous les composants installés sur chaque nœud IaaS, puis localisez l'agent de gestion IaaS.

d Vérifiez que la version de l'agent de gestion est à jour.

- [Exclure la mise à niveau d'laaS.](#)
- Vérifiez que la sauvegarde de la base de données laaS Microsoft SQL Server est accessible au cas où vous devriez procéder à une restauration.
- Vérifiez que les snapshots des serveurs laaS de votre déploiement sont disponibles.

Si la mise à niveau échoue, revenez au snapshot et à la sauvegarde de la base de données, puis tentez une autre mise à niveau.

Procédure

- 1 Ouvrez une nouvelle session de console sur l'hôte dispositif vRealize Automation. Connectez-vous avec le compte racine.
- 2 Passez au répertoire `/usr/lib/vcac/tools/upgrade/`.

Il est important que tous les agents de gestion laaS soient mis à niveau et dépourvus de défauts avant d'exécuter le script shell `./upgrade`. Si un agent de gestion laaS rencontre un problème lors de l'exécution du script shell de mise à niveau, reportez-vous à [La mise à jour ne réussit pas à mettre à jour l'agent de gestion](#).

- 3 Exécutez le script de mise à niveau.
 - a À l'invite de commandes, entrez `./upgrade`.
 - b Appuyez sur Entrée.

Pour une description du processus de mise à niveau d'laaS, reportez-vous à [Mise à jour du dispositif vRealize Automation et des composants laaS](#).

Si le script shell de mise à niveau échoue, vérifiez le fichier `upgrade-iaas.log`.

Vous pouvez réexécuter le script de mise à niveau après la correction d'un problème.

Étape suivante

- 1 [Rétablir l'accès au centre de contrôle vRealize Orchestrator intégré.](#)
- 2 Si votre déploiement utilise un équilibrage de charge, réactivez les moniteurs de santé vRealize Automation et le trafic vers tous les nœuds.

Pour plus d'informations, reportez-vous aux liens *Équilibrage de charge de vRealize Automation* dans la [documentation du produit vRealize Automation](#).

Mise à niveau des composants laaS à l'aide du fichier exécutable du programme d'installation d'laaS après la mise à niveau du dispositif vRealize Automation

Vous pouvez utiliser cette autre méthode pour mettre à niveau les composants laaS après la mise à niveau du dispositif vRealize Automation 7.1 ou version ultérieure.

Télécharger le programme d'installation d'laaS pour mettre à niveau les composants laaS après la mise à niveau du dispositif vRealize Automation

Après la mise à niveau du dispositif vRealize Automation vers la version cible, téléchargez le programme d'installation d'laaS sur la machine où les composants laaS devant être mis à niveau sont installés.

Si des avertissements de certificat s'affichent pendant cette procédure, vous pouvez les ignorer.

Note À l'exception d'une instance de sauvegarde passive du service du gestionnaire, le type de démarrage de tous les services doit être défini sur Automatique pendant le processus de mise à niveau. Le processus de mise à niveau ne parvient pas à définir des services sur Manuel.

Conditions préalables

- Vérifiez que Microsoft .NET Framework 4.5.2 ou une version ultérieure est installé sur la machine d'installation d'laaS. Vous pouvez télécharger le programme d'installation .NET à partir de la page Web du programme d'installation vRealize Automation. Si vous mettez à jour .NET vers la version 4.5.2 après avoir arrêté les services, et si la machine a redémarré dans le cadre de l'installation, il vous faut arrêter manuellement tous les services laaS, à l'exception de l'agent de gestion.
- Vérifiez que la fonctionnalité d'activation non-HTTP de .NET 3.5 Framework est configurée. La mise à niveau de vRealize Automation échoue si la fonctionnalité d'activation non-HTTP de .NET 3.5 Framework n'est pas configurée sur tous les nœuds laaS (Web, Manager Service, agent proxy, DEM). L'échec se produit si l'outil de vérification des conditions préalables ne dispose pas d'un accès à Internet pour télécharger et installer la version .NET la plus récente. Pour ajouter cette fonctionnalité :
 - a Ouvrez l'**assistant Ajouter des rôles et des fonctionnalités**.
 - b Sélectionnez **Fonctionnalités de .NET Framework 3.5**.
 - c Cochez la case **Activation Non-HTTP**.
- Si vous utilisez Internet Explorer pour le téléchargement, vérifiez que l'option de configuration de sécurité renforcée n'est pas activée. Entrez `res://iesetup.dll/SoftAdmin.htm` dans la barre de recherche et appuyez sur Entrée.
- Connectez-vous en tant qu'administrateur local au serveur Windows. Le serveur Windows est celui où un ou plusieurs des composants laaS que vous souhaitez mettre à niveau sont installés.

Procédure

- 1 Dans un navigateur, ouvrez la page d'installation d'laaS sur le dispositif vRealize Automation principal ou master.
<https://vrealize-automation-appliance-FQDN:5480/installer>
- 2 Cliquez sur **Programme d'installation d'laaS**.

- 3 Lorsque vous y êtes invité, enregistrez le fichier `setup__vrealize-automation-appliance-FQDN@5480.exe` sur le poste de travail.

Ne modifiez pas le nom de fichier. Le nom associe l'installation au dispositif vRealize Automation approprié.

Étape suivante

[Mettre à niveau les composants IaaS après la mise à niveau de vRealize Automation vers la version cible.](#)

Mettre à niveau les composants IaaS après la mise à niveau de vRealize Automation vers la version cible

Vous devez mettre à niveau la base de données SQL et configurer tous les systèmes sur lesquels des composants IaaS sont installés. Vous pouvez suivre ces étapes pour les installations minimales et distribuées.

Note Le programme d'installation d'IaaS doit se trouver sur la machine qui contient les composants IaaS que vous souhaitez mettre à niveau. Vous ne pouvez pas exécuter le programme d'installation depuis un emplacement externe, sauf pour la base de données Microsoft SQL qui peut également être mise à niveau à distance depuis le nœud Web.

Vérifiez que les snapshots des serveurs IaaS de votre déploiement sont disponibles. Si la mise à niveau échoue, vous pouvez revenir au snapshot et essayez une nouvelle fois de procéder à la mise à niveau.

Effectuez la mise à niveau afin que les services soient mis à niveau selon l'ordre suivant :

1 Sites Web IaaS

Si vous utilisez un équilibrage de charge, désactivez le trafic vers tous les nœuds non principaux.

Terminez la mise à niveau sur un serveur avant de réaliser la mise à niveau du prochain serveur exécutant un service de site Web. Commencez par celui sur lequel le composant Model Manager Data est installé.

Si vous effectuez une mise à niveau manuelle de la base de données Microsoft SQL externe, vous devez mettre à niveau la machine SQL externe avant de mettre à niveau le nœud Web. Vous pouvez mettre à niveau le SQL externe à distance à partir du nœud Web.

2 Manager Services

Mettez à niveau l'instance de Manager Service active avant de mettre à niveau l'instance de Manager Service passive.

Si le chiffrement SSL n'est pas activé dans votre instance de SQL, décochez la case Chiffrement SSL dans la boîte de dialogue Configuration de mise à niveau IaaS en regard de la définition de SQL.

3 DEM Orchestrator et DEM Workers

Mettez à niveau tous les DEM Orchestrator et les DEM Workers. Terminez la mise à niveau sur un serveur avant de réaliser la mise à niveau du prochain serveur.

4 Agents

Terminez la mise à niveau sur un serveur avant de réaliser la mise à niveau du prochain exécutant un agent.

5 Agent de gestion

Est mis à jour automatiquement lors de la procédure de mise à niveau.

Si vous utilisez différents services sur un serveur, la mise à niveau met à jour les services dans le bon ordre. Par exemple, si le site web et le composant Manager Service de votre site se trouvent sur le même serveur, veuillez les sélectionner les deux pour la mise à jour. Le programme d'installation de la mise à niveau effectue les mises à jour dans le bon ordre. Vous devez terminer la mise à niveau sur un serveur avant de commencer la mise à niveau d'un autre serveur.

Note Si votre déploiement utilise un équilibrage de charge, le dispositif principal doit être connecté à l'équilibrage de charge. Le trafic d'équilibrage de charge doit être désactivé pour toutes les autres instances des dispositifs vRealize Automation avant que vous appliquiez la mise à niveau pour éviter les erreurs de mise en cache.

Conditions préalables

- Sauvegardez votre environnement vRealize Automation existant.
- Si vous redémarrez un serveur IaaS après avoir mis à jour tous les dispositifs vRealize Automation, mais avant la mise à niveau des composants IaaS, arrêtez tous les services Windows IaaS sur le serveur, sauf le service Agent de gestion.
- [Télécharger le programme d'installation d'IaaS pour mettre à niveau les composants IaaS après la mise à niveau du dispositif vRealize Automation.](#)
- Vérifiez que l'environnement d'exécution JAVA SE 8, 64 bits, update 181 ou version ultérieure est installé sur votre site Web IaaS principal, la base de données Microsoft SQL et le nœud Model Manager. Après avoir installé Java, vous devez configurer la variable d'environnement JAVA_HOME à la nouvelle version sur chaque nœud de serveur.
- Vérifiez que la date de création est antérieure à la date de modification dans le fichier `web.config`. Si la date de création du fichier `web.config` est identique ou ultérieure à la date de modification, suivez la procédure décrite dans [Échec de la mise à niveau pour le composant de site Web IaaS](#).

- Répétez ces étapes pour reconfigurer le Coordinateur de transactions distribuées (DTC) Microsoft.

Note Même lorsque le Coordinateur de transactions distribuées est activé, la transaction distribuée peut échouer si le pare-feu est activé.

- a Sur le dispositif vRealize Automation, sélectionnez **Démarrer > Outils d'administration > Services composants**.
- b Développez **Services composants > Ordinateurs > Mon ordinateur > Coordinateur de transactions distribuées**.
- c Choisissez la tâche appropriée.
 - Pour un DTC local autonome, cliquez avec le bouton droit sur **DTC Local** et sélectionnez **Propriétés**
 - Pour un DTC en cluster, développez **DTC en cluster** et faites un clic droit sur le DTC en cluster nommé, puis sélectionnez l'option **Propriétés**.
- d Cliquez sur **Sécurité**.
- e Sélectionnez toutes les options suivantes.
 - **Accès DTC réseau**
 - **Autoriser les clients distants**
 - **Autoriser les transactions entrantes**
 - **Autoriser les transactions sortantes**
 - **Authentification mutuelle requise**
- f Cliquez sur **OK**.

Procédure

- 1 Si vous utilisez un équilibrage de charge, préparez votre environnement.
 - a Vérifiez que le nœud du site Web IaaS qui contient Model Manager Data est activé pour le trafic d'équilibrage de charge.

Vous pouvez identifier ce nœud par la présence du dossier `vCAC Folder\Server\ConfigTool`.
 - b Désactivez tous les autres sites Web IaaS et le composant Manager Services non principal pour le trafic de l'équilibrage de charge.
- 2 Cliquez avec le bouton droit sur le fichier d'installation `setup__vrealize-automation-appliance-FQDN@5480.exe` et sélectionnez **Exécuter en tant qu'administrateur**.
- 3 Cliquez sur **Suivant**.
- 4 Acceptez le contrat de licence, puis cliquez sur **Suivant**.

- 5 Saisissez les informations d'identification de l'administrateur pour le déploiement actif sur la page de connexion.

Le nom d'utilisateur est **root** et le mot de passe est celui que vous avez spécifié lorsque vous avez déployé le dispositif.

- 6 Sélectionnez **Accepter le certificat**.

- 7 Sur la page **Type d'installation**, vérifiez que **Mise à niveau** est sélectionné.

Si **Mise à niveau** n'est pas sélectionné, les composants de ce système sont déjà mis à niveau vers cette version.

- 8 Cliquez sur **Suivant**.

- 9 Configurez les paramètres de mise à niveau.

Option	Action
Si vous réalisez une mise à niveau de Model Manager Data	Sélectionnez la case Model Manager Data dans la section Serveur vCAC. La case est cochée par défaut. Effectuez la mise à niveau de Model Manager Data une seule fois. Si vous exécutez le fichier de configuration sur plusieurs machines pour mettre à niveau une installation distribuée, les serveurs Web interrompent leur fonctionnement tant que les versions de serveurs Web et de Model Manager Data sont différentes. Lors que la mise à niveau est terminée pour Model Manager Data et pour tous les serveurs Web, le fonctionnement de ces derniers reprend.
Si vous n'effectuez pas de mise à niveau de Model Manager Data	Désélectionnez la case Model Manager Data dans la section Serveur vCAC.
Pour conserver les workflows personnalisés à la dernière version dans votre Model Manager Data	Si vous mettez à niveau Model Manager Data, sélectionnez la case Conserver mes versions de workflow les plus récentes dans la section Workflows d'extensibilité. La case est cochée par défaut. Les workflows personnalisés sont toujours préservés. La case détermine uniquement l'ordre des versions. Si vous avez utilisé vRealize Automation Designer pour personnaliser les workflows dans Model Manager, sélectionnez cette option pour conserver la version la plus récente de chaque workflow personnalisé avant la mise à niveau comme la version la plus récente une fois la mise à niveau effectuée. Si vous ne sélectionnez pas cette option, la version de chaque workflow fournie avec vRealize Automation Designer devient la plus récente après la mise à niveau et la version la plus récente avant la mise à niveau devient la deuxième. Pour plus d'informations sur vRealize Automation Designer, reportez-vous à Extension de la durée des cycles de vie de la machine en utilisant vRealize Automation Designer .

Option	Action
Si vous effectuez une mise à niveau d'un Distributed Execution Manager ou d'un agent de proxy	Saisissez les informations d'identification pour le compte d'administration dans la section Compte du service. Tous les services que vous mettez à niveau sont exécutés dans ce compte.
Pour spécifier votre base de données Microsoft SQL Server	Si vous mettez à niveau Model Manager Data, saisissez les nom du serveur et de l'instance de la base de données dans le champ de texte Serveur dans la section Informations d'installation de la base de données Microsoft SQL Server. Entrez un nom de domaine complet (FQDN) pour le nom de serveur de la base de données dans le champ de texte Nom de la base de données . Si l'instance de la base de données ne correspond pas à un port SQL par défaut, il vous faut inclure le numéro de port dans la spécification de l'instance de serveur. Le numéro de port Microsoft SQL par défaut est 1433. Lorsque vous mettez à niveau les nœuds du gestionnaire, l'option MSSQL SSL est sélectionnée par défaut. Si votre base de données n'utilise pas SSL, décochez la case Utiliser SSL pour la connexion de la base de données .

10 Cliquez sur **Suivant**.

11 Confirmez que tous les services à mettre à niveau s'affichent sur la page Prêt pour la mise à niveau, puis cliquez sur **Mettre à niveau**.

La page Mise à niveau et un indicateur de progression s'affichent. Lorsque la procédure de mise à niveau se termine, le bouton **Suivant** est activé.

12 Cliquez sur **Suivant**.

13 Cliquez sur **Terminer**.

14 Vérifiez que tous les services ont redémarré.

15 Répétez ces étapes pour chaque serveur IaaS de votre déploiement dans l'ordre recommandé.

16 Une fois tous les composants mis à niveau, connectez-vous à l'interface de gestion du dispositif vRealize Automation et vérifiez que tous les services, y compris IaaS, sont désormais enregistrés.

17 (Facultatif) Activez le basculement automatique de Manager Service. Reportez-vous à [Activer le basculement automatique de Manager Service après une mise à niveau](#).

Résultats

Tous les composants sélectionnés sont mis à niveau vers la nouvelle version.

Étape suivante

- 1 [Rétablir l'accès au centre de contrôle vRealize Orchestrator intégré](#).
- 2 Si votre déploiement utilise un équilibrage de charge, mettez à niveau chaque nœud de l'équilibrage de charge pour utiliser les contrôles de santé vRealize Automation et réactivez le trafic de l'équilibrage de charge pour tous les nœuds non connectés.

Pour obtenir plus d'informations, reportez-vous à la section *Équilibrage de charge vRealize Automation*.

Rétablir l'accès au centre de contrôle vRealize Orchestrator intégré

Après la mise à niveau des composants du serveur IaaS, vous devez restaurer l'accès à vRealize Orchestrator.

Lorsque vous procédez à la mise à niveau vers vRealize Automation, vous devez effectuer cette procédure pour intégrer la nouvelle fonctionnalité de contrôle d'accès basé sur les rôles. Cette procédure est écrite pour un environnement à haute disponibilité.

Conditions préalables

Prenez un snapshot de votre environnement vRealize Automation.

Procédure

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

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

- 2 Sélectionnez **Cluster**.

- 3 Identifiez les nœuds master et de réplica.

- 4 Sur chaque nœud de réplica, ouvrez une session SSH, connectez-vous en tant qu'administrateur et exécutez la commande suivante :

```
service vco-server stop && service vco-configurator stop
```

- 5 Sur le nœud master, ouvrez une session SSH, connectez-vous en tant qu'administrateur et exécutez la commande suivante :

```
rm /etc/vco/app-server/vco-registration-id
```

- 6 Sur le nœud master, passez au répertoire `/etc/vco/app-server /`.

- 7 Ouvrez le fichier `sso.properties`.

- 8 Si le nom de propriété `com.vmware.o11n.sso.admin.group.name` contient des espaces ou tout autre caractère Bash pouvant être accepté comme caractère spécial dans une commande Bash comme une apostrophe (') ou un symbole dollar (\$), procédez comme suit.

- a Copiez la ligne incluant la propriété `com.vmware.o11n.sso.admin.group.name` et entrez `AdminGroup` pour la valeur.
- b Ajoutez `#` au début de la ligne d'origine incluant la propriété `com.vmware.o11n.sso.admin.group.name` pour la mettre en commentaire.
- c Enregistrez et fermez le fichier `sso.properties`.

- 9 Exécutez la commande suivante :

```
vcac-vami vco-service-reconfigure
```

- 10 Ouvrez le fichier `sso.properties`. Si le fichier a été modifié, procédez comme suit.
 - a Supprimez le symbole `#` au début de la ligne d'origine incluant la propriété `com.vmware.o11n.sso.admin.group.name` pour annuler la mise en commentaire de la ligne.
 - b Supprimez la copie de la ligne incluant la propriété `com.vmware.o11n.sso.admin.group.name`.
 - c Enregistrez et fermez le fichier `sso.properties`.
- 11 Exécutez cette commande pour redémarrer le service `vco-server` :


```
service vco-server restart
```
- 12 Exécutez cette commande pour redémarrer le service `vco-configurator` :


```
service vco-configurator restart
```
- 13 Dans l'interface de gestion du dispositif vRealize Automation, cliquez sur **Services** et attendez que tous les services du nœud master soient ENREGISTRÉ.
- 14 Lorsque tous les services sont enregistrés, joignez les nœuds de réplica vRealize Automation au cluster vRealize Automation pour synchroniser la configuration de vRealize Orchestrator.

Étape suivante

[Migration d'une instance externe de vRealize Orchestrator après la mise à niveau de vRealize Automation.](#)

Migration d'une instance externe de vRealize Orchestrator après la mise à niveau de vRealize Automation

À partir de vRealize Orchestrator 7.5, vous ne pouvez plus mettre à niveau vos environnements vRealize Orchestrator externes. Pour mettre à niveau des environnements vRealize Orchestrator externes vers la dernière version, vous devez les migrer.

Note L'instance de vRealize Orchestrator intégrée dans vRealize Automation est automatiquement mise à niveau avec la mise à niveau de vRealize Automation. Si vous utilisez uniquement une instance intégrée de vRealize Orchestrator, aucune action n'est nécessaire.

La migration de vRealize Orchestrator transfère une configuration vRealize Orchestrator source externe vers votre environnement vRealize Orchestrator 7.5 récemment configuré. Tous les éléments existants, tels que les workflows, les actions, les éléments de configuration et de ressources, les modules, les tâches, les stratégies, les certificats, les plug-ins, etc., sont alors remplacés.

Il existe deux options pour la mise à niveau d'une instance externe de vRealize Orchestrator lorsque vous effectuez la migration vers la dernière version de vRealize Automation.

- Migrez votre instance externe de vRealize Orchestrator vers une autre instance externe de vRealize Orchestrator. Reportez-vous à [Migrer un serveur Orchestrator externe vers un environnement vRealize Orchestrator 7.5](#) dans la documentation de vRealize Orchestrator.
- Migrez votre serveur vRealize Orchestrator externe vers une instance intégrée de vRealize Orchestrator dans vRealize Automation. Reportez-vous à [Migrer un serveur Orchestrator externe vers un environnement vRealize Orchestrator 7.5](#) dans la documentation de vRealize Orchestrator.

Note La migration d'une instance intégrée de vRealize Orchestrator vers un environnement vRealize Orchestrator externe n'est pas prise en charge.

Activer vos équilibres de charge

Si votre déploiement utilise des équilibres de charge, réactivez les nœuds secondaires et les contrôles de santé, puis rétablissez les paramètres de délai d'expiration d'équilibrage de charge.

Les contrôles de santé de vRealize Automation varient selon la version. Pour plus d'informations, reportez-vous au *Guide de Configuration de l'équilibrage de charge vRealize Automation* dans la documentation de [VMware vRealize Automation](#).

Rétablissez les paramètres de délai d'expiration d'équilibrage de charge de 10 minutes à la valeur par défaut.

Tâches à réaliser après la mise à niveau de vRealize Automation

Après la mise à niveau de vRealize Automation 7.1 ou version ultérieure, vous devez effectuer les tâches requises après la mise à niveau.

Ne pas modifier le fuseau horaire vRealize Automation

Même si l'interface de gestion du dispositif vRealize Automation fournit une option pour la modifier, laissez toujours le fuseau horaire vRealize Automation défini sur Etc/UTC.

L'utilisation d'un fuseau horaire autre qu'Etc/UTC peut provoquer des erreurs inhabituelles telles que l'échec de migrations et des bundles de journaux qui ne contiennent pas les entrées provenant de tous les nœuds vRealize Automation.

L'option de l'interface de gestion du dispositif vRealize Automation que vous devez éviter se trouve sous **Système > Fuseau horaire**.

Mise à niveau des agents logiciels TLS 1.2

Après la mise à niveau de vRealize Automation, vous devez effectuer plusieurs tâches pour mettre à niveau les agents logiciels de votre environnement vRealize Automation 7.1 ou version ultérieure vers TLS 1.2.

À partir de vRealize Automation 7.4, Transport Layer Security (TLS) 1.2 est le seul protocole TLS pris en charge pour la communication des données entre vRealize Automation et votre navigateur.

Après la migration, vous devez mettre à niveau les modèles de machine virtuelle existants à partir de votre environnement vRealize Automation 7.1 ou version ultérieure ainsi que toutes les machines virtuelles existantes.

Mettre à jour les modèles de machine virtuelle vRealize Automation

Vous devez mettre à jour les modèles existants après la mise à niveau vers la version de vRealize Automation cible afin que les agents logiciels utilisent le protocole TLS 1.2.

L'agent invité et le code de démarrage de l'agent doivent être mis à jour dans les modèles à partir de la version de vRealize Automation source. Si vous utilisez une option de clone lié, vous devrez éventuellement remapper les modèles avec les machines virtuelles récemment créées et leurs snapshots.

Pour mettre à niveau vos modèles, effectuez les tâches suivantes :

- 1 Connectez-vous à vSphere.
- 2 Convertissez chaque modèle de la version de vRealize Automation source en machine virtuelle et mettez la machine sous tension.
- 3 Importez le programme d'installation du logiciel approprié et exécutez-le sur chaque machine virtuelle.
- 4 Convertissez à nouveau chaque machine virtuelle vers un modèle.

Utilisez cette procédure pour localiser le programme d'installation de logiciel pour Linux ou Windows.

Conditions préalables

Mise à niveau réussie vers la version de vRealize Automation cible.

Procédure

- 1 Démarrez un navigateur et ouvrez la page de démarrage du dispositif vRealize Automation cible en utilisant le nom de domaine complet du dispositif virtuel : `https://vra-va-hostname.domain.name`.
- 2 Cliquez sur **Page d'invité et d'agents logiciels**.
- 3 Suivez les instructions du programme d'installation de logiciel Linux ou Windows.

Étape suivante

[Identifier les machines virtuelles nécessitant une mise à niveau des agents logiciels.](#)

Identifier les machines virtuelles nécessitant une mise à niveau des agents logiciels

Vous pouvez utiliser le service de santé de vRealize Automation pour identifier les machines virtuelles qui nécessitent une mise à jour des agents logiciels vers TLS 1.2.

Vous pouvez utiliser le service de santé pour identifier les machines virtuelles nécessitant une mise à jour des agents logiciels vers TLS 1.2. Vous devez mettre à jour tous les agents logiciels de l'environnement vRealize Automation pour pouvoir effectuer les procédures de post-provisionnement, car elles nécessitent une communication sécurisée entre votre navigateur et vRealize Automation.

Conditions préalables

- Mise à niveau réussie vers la version vRealize Automation.
- Vous êtes connecté à la version vRealize Automation cible sur le dispositif virtuel principal en tant qu'administrateur de locataire.

Procédure

- 1 Cliquez sur **Administration > Santé**.
- 2 Cliquez sur **Nouvelle configuration**.
- 3 Sur la page Détails de la configuration, fournissez les renseignements demandés.

Option	Commentaire
Nom	Entrez Vérification des agents logiciels .
Description	Ajoutez une description facultative, par exemple, Recherche des agents logiciels à mettre à niveau vers TLS 1.2 .
Produit	Sélectionnez la version vRealize Automation que vous avez mise à niveau ou vers laquelle vous avez migré.
Planifier	Sélectionnez Aucun .

- 4 Cliquez sur **Suivant**.
- 5 Sur la page Sélectionner les suites de tests, sélectionnez **Tests système de vRealize Automation** et **Tests de locataire de vRealize Automation**.
- 6 Cliquez sur **Suivant**.
- 7 Sur la page Configurer les paramètres, fournissez les renseignements demandés.

Tableau 1-54. Dispositif virtuel vRealize Automation

Option	Description
Adresse du serveur Web public	<ul style="list-style-type: none"> ■ Pour un déploiement minimal, l'URL de base pour l'hôte du dispositif vRealize Automation. Par exemple, <code>https://va-host.domain/</code>. ■ Pour un déploiement haute disponibilité, l'URL de base de l'équilibrage de charge vRealize Automation. Par exemple, <code>https://load-balancer-host.domain/</code>.
Adresse de la console SSH	Nom de domaine complet du dispositif vRealize Automation. Par exemple, <code>va-host.domain</code> .
Utilisateur de la console SSH	root
Mot de passe de la console SSH	Mot de passe de l'utilisateur racine.
Temps de réponse maximal du service (ms)	Acceptez la valeur par défaut : 2 000

Tableau 1-55. Locataire système vRealize Automation

Option	Description
Administrateur du locataire système	administrateur
Mot de passe du locataire système	Mot de passe de l'administrateur.

Tableau 1-56. Surveillance de l'espace disque vRealize Automation

Option	Description
Pourcentage du seuil d'avertissement	Acceptez la valeur par défaut : 75
Pourcentage de seuil critique	Acceptez la valeur par défaut : 90

Tableau 1-57. Locataire vRealize Automation

Option	Description
Locataire en cours de test	Locataire sélectionné pour les tests.
Nom d'utilisateur administrateur Fabric	Nom d'utilisateur administrateur Fabric. Par exemple, admin@va-host.local. Note Cet administrateur Fabric doit également disposer des rôles d'administrateur de locataire et d'administrateur IaaS pour pouvoir exécuter l'ensemble des tests.
Mot de passe administrateur Fabric	Mot de passe administrateur Fabric.

- 8 Cliquez sur **Suivant**.
- 9 Sur la page Résumé, passez en revue les informations, puis cliquez sur **Terminer**.
La configuration de la vérification des agents logiciels est terminée.
- 10 Sur la carte de vérification des agents logiciels, cliquez sur **Exécuter**.
- 11 Lorsque le test est terminé, cliquez au centre de la carte de vérification des agents logiciels.
- 12 Sur la page de résultats de la vérification des agents logiciels, parcourez les résultats des tests et recherchez le test Rechercher la version des agents logiciels dans la colonne Nom. Si le résultat du test est Échec, cliquez sur le lien **Cause** dans la colonne Cause pour afficher les machines virtuelles qui comportent un agent logiciel obsolète.

Étape suivante

Si tel est le cas, reportez-vous à la section [Mettre à niveau les agents logiciels sur vSphere](#).

Mettre à niveau les agents logiciels sur vSphere

Après la mise à niveau, vous pouvez mettre à niveau les agents logiciels obsolètes sur vSphere vers TLS 1.2 à l'aide de la gestion des dispositifs vRealize Automation.

Cette procédure met à jour les agents logiciels obsolètes vers TLS 1.2 sur les machines virtuelles de votre environnement mis à niveau. Elle est requise pour effectuer la mise à niveau vers la version de vRealize Automation cible.

Conditions préalables

- Mise à niveau réussie vers la version de vRealize Automation cible.
- Vous avez utilisé le service de santé pour identifier les dispositifs virtuels comportant des agents logiciels obsolètes.

Procédure

- 1 Sur votre dispositif vRealize Automation principal, connectez-vous à la gestion des dispositifs vRealize Automation en tant qu'utilisateur **racine** à l'aide du mot de passe que vous avez entré lorsque vous avez déployé le dispositif vRealize Automation.

Pour un environnement haute disponibilité, ouvrez la gestion des dispositifs sur le dispositif principal.

- 2 Cliquez sur **vRA > Agents logiciels**.
- 3 Cliquez sur **Activer/désactiver TLS 1.0, 1.1**.

L'état de TLS v1.0, v1.1 est ACTIVÉ.

- 4 En ce qui concerne les informations d'identification du locataire, entrez les informations demandées pour le dispositif vRealize Automation cible.

Option	Description
Nom du locataire	Nom du locataire sur le dispositif vRealize Automation mis à niveau. Note L'utilisateur du locataire doit avoir le rôle d'architecte de logiciel.
Nom d'utilisateur	Nom d'utilisateur administrateur du locataire sur le dispositif vRealize Automation.
Mot de passe	Mot de passe administrateur du locataire.

- 5 Cliquez sur **Tester la connexion**.

Si une connexion est établie, un message de réussite s'affiche.

- 6 Cliquez sur **Répertorier les lots**.

Le tableau Liste de choix des lots apparaît.

- 7 Cliquez sur **Afficher**.

Un tableau apparaît avec une liste des machines virtuelles comportant des agents logiciels obsolètes.

8 Mettez à niveau l'agent logiciel des machines virtuelles présentant l'état **POUVANT ÊTRE MIS À NIVEAU**.

- Pour mettre à niveau l'agent logiciel d'une machine virtuelle individuelle, cliquez sur **Afficher** pour un groupe de machines virtuelles, identifiez la machine virtuelle que vous souhaitez mettre à niveau, puis cliquez sur **Exécuter** pour démarrer la mise à niveau.
- Pour mettre à niveau l'agent logiciel d'un lot de machines virtuelles, identifiez le groupe que vous souhaitez mettre à niveau, puis cliquez sur **Exécuter** pour démarrer la mise à niveau.

Si vous disposez de plus de 200 machines virtuelles à mettre à niveau, vous pouvez contrôler la vitesse de mise à niveau du lot en entrant des valeurs pour ces paramètres.

Option	Description
Taille du lot	Nombre de machines virtuelles sélectionnées pour la mise à niveau du lot. Vous pouvez modifier ce nombre pour régler la vitesse de mise à niveau.
Profondeur de file d'attente	Nombre d'exécutions parallèles de la mise à niveau qui s'exécutent en même temps. Par exemple, 20. Vous pouvez modifier ce nombre pour régler la vitesse de mise à niveau.
Erreurs du lot	Nombre d'erreurs REST entraînant le ralentissement de la mise à niveau du lot. Par exemple, si vous souhaitez arrêter la mise à niveau du lot en cours après 5 échecs afin d'améliorer la stabilité de la mise à niveau, entrez 5 dans le champ de texte.
Échecs du lot	Nombre d'échecs de mise à niveau des agents logiciels entraînant le ralentissement du traitement du lot. Par exemple, si vous souhaitez arrêter la mise à niveau du lot en cours après 5 échecs afin d'améliorer la stabilité de la mise à niveau, entrez 5 dans le champ de texte.
Interrogation du lot	Fréquence d'interrogation de la mise à niveau pour vérifier l'état du processus. Vous pouvez modifier ce nombre pour régler la vitesse de mise à niveau.

Si le processus de mise à niveau est trop lent ou génère trop de mises à niveau infructueuses, vous pouvez ajuster ces paramètres afin d'améliorer les performances de la mise à niveau.

Note Cliquer sur **Actualiser** permet d'effacer la liste des lots. Cela n'affecte rien le processus de mise à niveau. Cliquer sur **Actualiser** permet également d'actualiser les informations indiquant si TLS 1.2 est défini ou pas, mais aussi d'effectuer un contrôle de santé des services vRealize Automation. Si les services ne sont pas en cours d'exécution, un message d'erreur s'affiche et tous les autres boutons d'action sont désactivés.

9 Cliquez sur **Activer/désactiver TLS 1.0, 1.1**.

L'état de TLS v1.0, v1.1 est **DÉSACTIVÉ**.

Mettre à niveau les agents logiciels sur Amazon Web Service ou Azure

Vous pouvez mettre à niveau manuellement tous les agents logiciels obsolètes installés sur des machines virtuelles sur Amazon Web Services (AWS) ou Azure.

Conditions préalables

- Mise à niveau réussie vers votre version de vRealize Automation cible.
- Un tunnel de logiciel est présent et l'adresse IP du tunnel de la machine virtuelle est connue.

Procédure

- 1 Créez un fichier de nœud pour chaque nœud que vous devez mettre à niveau.

```
/usr/lib/vcac/server/webapps/ROOT/software/initializeUpdateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -tu <$TenantUser> -S <$SourceVRAServer>
```

Note Pour une mise à niveau sur place, \$DestinationVRAServer est identique à \$SourceVRAServer.

- 2 Créez un fichier de plan pour mettre à niveau l'agent logiciel sur une machine virtuelle Linux ou Windows.
 - Modifiez le fichier migrate params sous /var/log/vcac/agentupdate/{tenant}/{subtenant-UUID} afin qu'il contienne la valeur de l'adresse IP privée correspondant au point de terminaison AWS ou Azure.

```
"key": "ipAddress",
  "value": {
    "type": "string",
    "value": "<$PrivateIp:$PrivatePort>"
  }
}
```

- Utilisez cette commande pour mettre à jour une machine Linux.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CL
Software.LinuxAgentUpdateversion --source_cloud_provider azure
```

- Utilisez cette commande pour mettre à jour une machine Windows.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CW
Software.WindowsAgentUpdateversion --source_cloud_provider azure
```

- Cette commande exécute le fichier de plan.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -tu <$TenantUser> --plan_file /usr/lib/vcac/server/
webapps/ROOT/software/plan
```

- 3 Utilisez-la pour mettre à jour l'agent logiciel au moyen du fichier de nœud de l'étape 1 et du fichier de plan de l'étape 2.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer> -t <
$tenant> -tu <$TenantUser> --component_windows Software.WindowsAgentUpdateversion --
component_linux Software.LinuxAgentUpdate74 --plan_file /usr/lib/vcac/server/webapps/ROOT/
software/plan --plan_index 0 --node_file /usr/lib/vcac/server/webapps/ROOT/software/node --
source_cloud_provider azure --action plan_batch -S <$SourceVRAServer>
```

Vous pouvez aussi l'utiliser pour exécuter un seul nœud à la fois depuis le fichier de nœud en fournissant un index de nœud.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer> -t <
$tenant> -tu <$TenantUser> --component_windows Software.WindowsAgentUpdateversion --
component_linux Software.LinuxAgentUpdate74 --plan_file /usr/lib/vcac/server/webapps/ROOT/
software/plan --plan_index 0 --node_file /usr/lib/vcac/server/webapps/ROOT/software/node --
source_cloud_provider azure --action execute_node -S <$SourceVRAServer> --node_index <0 through
n-1>
```

Lorsque vous effectuez cette procédure, vous pouvez suivre les journaux provenant du dispositif virtuel et de la machine hôte vRealize Automation afin de voir le processus de mise à niveau des agents serveur.

Après la mise à niveau, le processus de mise à niveau importe un script de mise à jour logicielle pour Windows ou Linux dans le dispositif virtuel vRealize Automation. Vous pouvez vous connecter à l'hôte du dispositif virtuel vRealize Automation pour vous assurer que le composant logiciel a été correctement importé. Une fois le composant importé, une mise à jour logicielle est envoyée à l'ancien service EBS (Event Broker Service) pour qu'il relaye les scripts de mise à jour logicielle aux machines virtuelles identifiées. Une fois la mise à niveau terminée et les nouveaux agents logiciels opérationnels, une liaison est établie avec le nouveau dispositif virtuel vRealize Automation via l'envoi d'une demande ping.

Note Fichiers journaux utiles

- Sortie Catalina de la source vRealize Automation : /var/log/vcac/catalina.out. Ce fichier affiche les demandes de mise à niveau effectuées au fur et à mesure de la migration des agents. Cette activité est identique à la demande de provisionnement d'un logiciel en cours d'exécution.
- Sortie Catalina de la destination vRealize Automation : /var/log/vcac/catalina.out. Ce fichier affiche les machines virtuelles migrées en indiquant leurs demandes ping avec les numéros de version *version.0-SNAPSHOT*. Vous pouvez faire concorder ces informations en comparant les noms de rubrique EBS, par exemple, sw-agent-UUID.

- Dossier de mise à jour des agents sur le fichier journal de mise à niveau principal de la machine vRealize Automation de destination : `/var/log/vmware/vcac/agentupdate/updateSoftwareAgents.log`. Vous pouvez suivre ce fichier pour afficher les opérations de mise à niveau en cours.
- Journaux individuels disponibles sous les dossiers du locataire : `/var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}`. Les nœuds individuels y sont répertoriés en tant que fichiers du lot, avec les échecs et les extensions en cours.
- Machines virtuelles migrées : `/opt/vmware-appdirector/agent/logs/darwin*.log`. Vous pouvez vérifier cet emplacement de manière ponctuelle. Il doit indiquer les demandes de mises à jour logicielles en cours de réception ainsi que le redémarrage éventuel de l'agent de démarrage et de l'agent logiciel.

Définir le mode de réplication PostgreSQL vRealize Automation sur Synchron

Si vous définissez le mode de réplication PostgreSQL sur Asynchrone avant de procéder à la mise à niveau, vous pouvez définir le mode de réplication PostgreSQL sur Synchron après la mise à niveau d'un environnement vRealize Automation distribué.

Conditions préalables

Vous avez mis à niveau un environnement vRealize Automation distribué.

Procédure

- 1 Connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Cliquez sur **Cluster**.
- 3 Cliquez sur **Mode de synchronisation** et attendez la fin de l'action.
- 4 Vérifiez que tous les nœuds de la colonne État de synchronisation affichent le statut Synchronisation.

Étape suivante

[Exécuter l'action Tester la connexion et vérifier les points de terminaison mis à niveau.](#)

Exécuter l'action Tester la connexion et vérifier les points de terminaison mis à niveau

La mise à niveau effectuée à partir de versions antérieures de vRealize Automation apporte des modifications à certains points de terminaison dans l'environnement cible.

Après la mise à niveau vers vRealize Automation, vous devez utiliser l'action **Tester la connexion** pour tous les points de terminaison applicables. Vous devrez également ajuster certains points de terminaison mis à niveau. Pour plus d'informations, reportez-vous à la section [Considérations lors de l'utilisation de points de terminaison mis à niveau ou migrés](#).

Le paramètre de sécurité par défaut pour les points de terminaison mis à niveau ou migrés consiste à ne pas accepter les certificats non approuvés.

Après la mise à niveau ou la migration à partir d'une version antérieure à vRealize Automation, si vous utilisez des certificats non approuvés, vous devez effectuer la procédure suivante pour tous les points de terminaison vSphere et NSX afin d'activer la validation du certificat. Si vous ne le faites pas, les opérations de point de terminaison échouent et produisent des erreurs de certificat. Pour plus d'informations, consultez les articles de la base de connaissances VMware *La communication au point de terminaison est interrompue après la mise à niveau vers vRA 7.3* (2150230) à l'adresse <http://kb.vmware.com/kb/2150230> et *Comment télécharger et installer des certificats vCenter Server racine pour éviter les avertissements de certificat de navigateur Web* (2108294) à l'adresse <http://kb.vmware.com/kb/2108294>.

- 1 Après une mise à niveau ou une migration, connectez-vous à la machine de l'agent vSphere/vRealize Automation et redémarrez vos agents vSphere à l'aide de l'onglet **Services**.

Il se peut que la migration ne fasse pas redémarrer tous les agents ; si tel est le cas, redémarrez-les manuellement.

- 2 Attendez qu'au moins un rapport de commande ping se termine. Cette opération peut prendre une à deux minutes.
- 3 Lorsque les agents vSphere ont démarré la collecte de données, connectez-vous à vRealize Automation en tant qu'administrateur laaS.
- 4 Cliquez sur **Infrastructure > Points de terminaison > Points de terminaison**.
- 5 Modifiez un point de terminaison vSphere et cliquez sur **Tester la connexion**.
- 6 Si une invite de certificat s'affiche, cliquez sur **OK** pour accepter le certificat.

Si aucune invite de certificat ne s'affiche, il se peut qu'actuellement le certificat soit correctement stocké dans une autorité racine approuvée du service d'hébergement de la machine Windows pour le point de terminaison, par exemple en tant que machine de l'agent proxy ou machine DEM.

- 7 Cliquez sur **OK** pour appliquer l'acceptation du certificat et enregistrer le point de terminaison.
- 8 Répétez cette procédure pour chaque point de terminaison vSphere.
- 9 Répétez cette procédure pour chaque point de terminaison NSX.
- 10 Accédez à **Infrastructure > Ressources de calcul**, cliquez avec le bouton droit sur votre ressource **vCenter Compute**, puis exécutez **Collecte de données**.

Si l'action **Tester la connexion** réussit, mais certaines opérations de collecte ou de provisionnement de données échouent, vous pouvez installer le même certificat sur toutes les machines de l'agent qui servent de point de terminaison et sur toutes les machines DEM. Vous pouvez également désinstaller le certificat des machines existantes et répéter la procédure précédente pour le point de terminaison défaillant.

Exécuter la collecte de données d'inventaire réseau et de sécurité NSX après la mise à niveau de vRealize Automation

Avant de migrer à partir de vRealize Automation, vous devez exécuter la collecte de données d'inventaire réseau et de sécurité NSX dans l'environnement vRealize Automation mis à niveau.

Cette tâche de collecte de données est nécessaire pour que l'option de reconfiguration d'équilibrage de charge soit prise en charge dans les déploiements.

Conditions préalables

- [Exécuter la collecte de données d'inventaire réseau et de sécurité NSX avant la mise à niveau de vRealize Automation.](#)
- Mettez à niveau vRealize Automation.

Procédure

- ◆ Exécutez la collecte de données d'inventaire réseau et de sécurité NSX dans vRealize Automation après la mise à niveau. Consultez [Démarrer la collecte de données de point de terminaison manuellement](#).

Joindre un dispositif de réplica à un cluster

Une fois la mise à jour du dispositif vRealize Automation master terminée, chaque nœud de réplica mis à jour rejoint automatiquement le nœud master. Lorsqu'un nœud de réplica doit être mis à jour séparément, ajoutez-le manuellement au cluster.

Procédure

- 1 Sur le nœud de réplica qui n'est pas joint au cluster, connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.

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

- 2 Sélectionnez **Cluster**.
- 3 Cliquez sur **Joindre un cluster**.

Configuration de port pour les déploiements à haute disponibilité

Après avoir terminé une mise à niveau dans un déploiement à haute disponibilité, il vous faut configurer l'équilibrage de charge pour faire passer le trafic du port 8444 vers le dispositif vRealize Automation pour prendre en charge les fonctionnalités de console distante.

Pour plus d'informations, reportez-vous au *Guide de configuration de l'équilibrage de charge de vRealize Automation* dans la [documentation de vRealize Automation](#).

Restaurer les fichiers de délai d'expiration du workflow externe

Vous devez reconfigurer les fichiers de délai d'expiration du workflow externe vRealize Automation, car la procédure de mise à niveau remplace les fichiers xmldb.

Procédure

- 1 Ouvrez les fichiers configuration (xmldb) du workflow externe sur votre système dans l'annuaire suivant.
`\VMware\VCAC\Server\ExternalWorkflows\xmldb\.`
- 2 Remplacez les fichiers xmldb par les fichiers que vous avez sauvegardés avant la migration. Si vous n'avez pas de fichiers de sauvegarde, reconfigurez les paramètres de délai d'expiration du workflow externe.
- 3 Enregistrez vos paramètres.

Restaurer les modifications apportées à la connexion dans le fichier app.config

Le processus de mise à niveau remplace les modifications que vous avez apportées à la connexion dans les fichiers de configuration. Après avoir procédé à une mise à niveau, vous devez restaurer toutes les modifications apportées au fichier app.config avant la mise à niveau.

Vous pouvez restaurer les modifications en effectuant une fusion sans remplacer les modifications apportées aux fichiers *.exe.config (par exemple, managervice.exe.config) sur votre serveur IaaS que vous avez sauvegardé lors des tâches prérequis.

Reconfiguration du point de terminaison Azure après la mise à niveau

Après la mise à niveau, vous devez reconfigurer le point de terminaison Microsoft Azure.

Effectuez cette procédure pour chaque point de terminaison Microsoft Azure.

Conditions préalables

- Mise à niveau réussie vers la version cible de vRealize Automation.
- Connectez-vous à la console vRealize Automation cible.
 - a Ouvrez la console vRealize Automation à l'aide du nom de domaine complet du dispositif virtuel cible : `https://vra-va-hostname.domain.name/vcac`.

Pour un environnement à haute disponibilité, ouvrez la console à l'aide du nom de domaine complet de l'équilibrage de charge du dispositif virtuel cible : `https://vra-va-lb-hostname.domain.name/vcac`.
 - b Connectez-vous en tant qu'utilisateur administrateur IaaS.

Procédure

- 1 Sélectionnez **Administration > Configuration vRO > Points de terminaison**.
- 2 Sélectionnez un point de terminaison Microsoft Azure.
- 3 Cliquez sur **Modifier**.
- 4 Cliquez sur **Détails**.
- 5 Sélectionnez la région dans le menu déroulant de l'environnement Azure.
- 6 Entrez la clé secrète client d'origine dans la zone de texte correspondante.

- 7 Entrez l'URL de stockage dans la zone de texte URI du stockage Azure.

Exemple : `https://mystorageaccount.blob.core.windows.net`

- 8 Cliquez sur **Terminer**.
- 9 Répétez pour chaque point de terminaison Azure.

Activer le basculement automatique de Manager Service après une mise à niveau

Le basculement automatique de Manager Service est désactivé par défaut lorsque vous effectuez une mise à niveau de vRealize Automation.

Appliquez cette procédure pour activer automatiquement Manager Service après la mise à niveau.

Procédure

- 1 Ouvrez une invite de commande en tant qu'utilisateur racine sur le dispositif vRealize Automation.
- 2 Changez les répertoires en `/usr/lib/vcac/tools/vami/commands`.
- 3 Pour activer le basculement automatique de Manager Service, exécutez la commande suivante.

```
python ./manager-service-automatic-failover ENABLE
```

Pour désactiver le basculement automatique dans un déploiement de IaaS, exécutez la commande suivante.

```
python ./manager-service-automatic-failover DISABLE
```

À propos du basculement automatique de Manager Service

Vous pouvez configurer Manager Service vRealize Automation IaaS pour basculer automatiquement sur une sauvegarde si l'instance principale de Manager Service s'arrête.

À partir de vRealize Automation 7.3, vous n'avez plus besoin de démarrer ou d'arrêter Manager Service manuellement sur chaque serveur Windows pour contrôler lequel est utilisé comme serveur principal ou de sauvegarde. Le basculement automatique de Manager Service est désactivé par défaut lorsque vous mettez à niveau IaaS à l'aide du script shell de mise à niveau ou du fichier exécutable du programme d'installation IaaS.

Lorsque le basculement automatique est activé, Manager Service démarre automatiquement sur tous les hôtes Manager Service, y compris les sauvegardes. La fonctionnalité de basculement automatique permet aux hôtes de se surveiller mutuellement de manière transparente et de basculer lorsque cela est nécessaire, mais le service Windows doit être en cours d'exécution sur tous les hôtes.

Note Vous n'êtes pas obligé d'utiliser le basculement automatique. Vous pouvez le désactiver et continuer de démarrer et d'arrêter manuellement le service Windows pour contrôler quel hôte sert d'hôte principal ou de sauvegarde. Si vous choisissez le basculement manuel, il vous suffit de démarrer le service sur un hôte à la fois. Avec le basculement automatique désactivé, l'exécution simultanée du service sur plusieurs serveurs IaaS rend vRealize Automation inutilisable.

Ne tentez pas d'activer ou de désactiver de manière sélective le basculement automatique. Le basculement automatique doit toujours être synchronisé, qu'il soit sous tension ou hors tension, sur chaque hôte Manager Service dans un déploiement IaaS.

Importer le plug-in DynamicTypes

Si vous utilisez le plug-in DynamicTypes et que vous avez exporté la configuration sous la forme d'un module avant la mise à niveau, vous devez importer le workflow suivant :

- 1 Importez la configuration de DynamicTypes dans l'environnement cible.
 - a Connectez-vous à Java Client en tant qu'utilisateur administrateur.
 - b Sélectionnez l'onglet **Workflows**.
 - c Sélectionnez **Bibliothèque > Types dynamiques > Configuration**.
 - d Sélectionnez le workflow **Importer la configuration en tant que module** et exécutez-le.
 - e Cliquez sur **Module de configuration à importer**.
 - f Accédez au fichier de module exporté, puis cliquez sur **Joindre un fichier**.
 - g Passez en revue les informations sur les espaces de nommage joints au module et cliquez sur **Envoyer**.
- 2 Sélectionnez **Inventaire > Types dynamiques** pour vérifier que les espaces de noms de type dynamique ont été importés.

Mise à niveau de VMware Identity Manager Connector

Après la mise à niveau de votre application vRealize Automation vers la version 7.5, vous devrez peut-être mettre à niveau le connecteur VMware Identity Manager (vIDM) externe pour l'authentification par carte à puce.

vRealize Automation 7.5 nécessite la version matérielle 3.1 ou ultérieure. Pour plus d'informations sur la mise à niveau vers la dernière version de vIDM, reportez-vous à la [documentation de VMware Identity Manager](#).

Note Si la version de votre connecteur vIDM est 2.7 ou une version antérieure, vous devez d'abord effectuer une mise à niveau vers la version 2.8.3, puis une mise à niveau vers la version 3.1 ou version ultérieure.

Résolution des problèmes de mise à niveau de vRealize Automation

Les rubriques de dépannage de mise à niveau offrent des solutions aux problèmes que vous pouvez rencontrer lors de la mise à niveau de vRealize Automation 7.1 ou version ultérieure.

Impossible d'activer le basculement automatique de Manager Service

Suggestions pour le dépannage de la commande `manager-service-automatic-failover`.

Solution

- ◆ La commande de basculement automatique de Manager Service échoue ou affiche le message suivant pendant plus de deux minutes : `Activation du mode de basculement automatique de Manager Service sur le nœud : IAAS_MANAGER_SERVICE_NODEID`.
 - a Connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.
`https://vrealize-automation-appliance-FQDN:5480`
 - b Sélectionnez **Cluster**.
 - c Vérifiez que le service de l'agent de gestion est en cours d'exécution sur tous les hôtes Manager Service.
 - d Vérifiez que la durée de la dernière connexion était inférieure à 30 secondes pour tous les nœuds IaaS Manager Service.

Si vous rencontrez des problèmes concernant la connectivité de l'agent de gestion, résolvez-les manuellement et relancez la commande pour activer le basculement automatique de Manager Service.

- ◆ La commande de basculement automatique de Manager Service ne parvient pas à activer le basculement sur un nœud Manager Service. Pour résoudre ce problème, il est recommandé de réexécuter la commande.
- ◆ Le basculement n'est activé que pour certains hôtes Manager Service inclus dans le déploiement IaaS. La fonctionnalité doit être activée sur tous les hôtes Manager Service inclus dans le déploiement IaaS. Pour résoudre ce problème, procédez de l'une des manières suivantes :
 - Désactivez le basculement sur tous les nœuds Manager Service et utilisez la méthode de basculement manuel à la place. Exécutez le basculement uniquement sur un hôte à la fois.

- Si, après plusieurs tentatives, vous ne parvenez toujours pas à activer la fonctionnalité sur un nœud Manager Service, arrêtez le service Windows VMware vCloud Automation Center sur ce nœud et définissez le type de démarrage du nœud sur Manuel pour résoudre le problème.
- ◆ Utilisation Python pour valider que le basculement est activé sur chaque nœud Manager Service.
 - a Connectez-vous au nœud du dispositif vRealize Automation master en tant qu'utilisateur **racine** via SSH.
 - b Exécutez `python /usr/lib/vcac/tools/vami/commands/manager-service-automatic-failover ENABLE`.
 - c Vérifiez que le système renvoie le message suivant : Activation du mode de basculement automatique de Manager Service sur le nœud : `IAAS_MANAGER_SERVICE_NODEID` effectuée.
- ◆ Confirmez que le basculement est activé sur chaque nœud Manager Service en consultant le fichier de configuration de Manager Service.
 - a Ouvrez une invite de commande sur un nœud Manager Service.
 - b Accédez au dossier d'installation de vRealize Automation et ouvrez le fichier de configuration de Manager Service sous `VMware\VCAC\Server\ManagerService.exe.config`.
 - c Vérifiez que les éléments suivants figurent dans la section `<appSettings>`.
 - `<add key="FailoverModeEnabled" value="True" />`
 - `<add key="FailoverPingIntervalMilliseconds" value="30000" />`
 - `<add key="FailoverNodeState" value="active" />`
 - `<add key="FailoverMaxFailedDatabasePingAttempts" value="5" />`
 - `<add key="FailoverMaxFailedRepositoryPingAttempts" value="5" />`
- ◆ Vérifiez que l'état du service Windows VMware vCloud Automation Center est Démarré et que le type de démarrage est défini sur Automatique.
- ◆ Utilisation Python pour valider que le basculement est désactivé sur chaque nœud Manager Service.
 - a Connectez-vous au nœud du dispositif vRealize Automation master en tant qu'utilisateur **racine** via SSH.
 - b Exécutez `python /usr/lib/vcac/tools/vami/commands/manager-service-automatic-failover DISABLE`.
 - c Vérifiez que le système renvoie le message suivant : Désactivation du mode de basculement automatique de Manager Service sur le nœud : `IAAS_MANAGER_SERVICE_NODEID` effectuée.

- ◆ Confirmez que le basculement est désactivé sur chaque nœud Manager Service en consultant le fichier de configuration de Manager Service.
 - a Ouvrez une invite de commande sur un nœud Manager Service.
 - b Accédez au dossier d'installation de vRealize Automation et ouvrez le fichier de configuration de Manager Service sous `VMware\vmcac\Server\ManagerService.exe.config`.
 - c Vérifiez que l'élément suivant figure dans la section `<appSettings>`.
 - `<add key="FailoverModeEnabled" value="False" />`
- ◆ Pour créer un nœud Manager Service de veille à froid, définissez l'état du nœud du service Windows VMware vCloud Automation Center sur Arrêté et le type de démarrage sur Manuel.
- ◆ Pour un nœud Manager Service actif, l'état du nœud du service Windows VMware vCloud Automation Center doit être Démarré et le type de démarrage doit être automatique.
- ◆ La commande de basculement automatique de Manager Service utilise l'ID interne du nœud Manager Service : `IAAS_MANAGER_SERVICE_NODEID`. Pour trouver le nom d'hôte correspondant à cet ID interne, exécutez la commande `vra-command list-nodes` et recherchez l'hôte Manager Service avec l'ID de nœud : `IAAS_MANAGER_SERVICE_NODEID`.
- ◆ Pour rechercher l'hôte Manager Service défini automatiquement comme actif par le système, procédez comme suit.
 - a Connectez-vous au nœud du dispositif vRealize Automation master en tant qu'utilisateur **racine** via SSH.
 - b Exécutez `vra-command list-nodes --components`.
 - Si le basculement est activé, recherchez le nœud Manager Service à l'état Actif.
 - Si le basculement est désactivé, recherchez le nœud Manager Service à l'état Démarré.

L'installation des mises à niveau échoue avec une erreur de délai d'attente des équilibrages de charge

Une installation ou une mise à niveau de vRealize Automation pour un déploiement distribué avec un équilibrage de charge échoue et renvoie une erreur de service 503 non disponible.

Problème

L'installation ou la mise à niveau échoue, car le paramètre d'expiration de l'équilibrage de charge n'accorde pas suffisamment de temps pour l'exécution de la tâche.

Cause

Un paramètre de délai d'expiration d'équilibrage de charge insuffisant peut entraîner un échec. Vous pouvez corriger le problème en augmentant le paramètre de délai d'expiration de l'équilibrage de charge à 100 secondes ou plus et en réexécutant la tâche.

Solution

- 1 Augmentez la valeur du délai d'expiration de l'équilibrage de charge à au moins 100 secondes.
- 2 Réexécutez l'installation ou la mise à niveau.

Échec de la mise à niveau pour le composant de site Web IaaS

La mise à niveau d'IaaS échoue et ne peut pas continuer.

Problème

La mise à niveau d'IaaS échoue pour le composant de site Web. Les messages d'erreur suivants s'affichent dans le fichier journal du programme d'installation.

- System.Data.Services.Client.DataServiceQueryException:
An error occurred while processing this request. --->
System.Data.Services.Client.DataServiceClientException: <!DOCTYPE html>
- **Description:** An application error
occurred on the server. The current custom error settings for this application prevent the details of the application error from being viewed remotely (for security reasons). It could, however, be viewed by browsers running on the local server machine.
- Warning: Non-zero return code. Command failed.
- Done Building Project "C:\Program Files
(x86)\VMware\VCAC\Server\Model Manager Data\DeployRepository.xml"
(InstallRepoModel target(s)) -- FAILED.

Les messages d'erreur suivants s'affichent dans le fichier journal de référentiel.

- [Error]: [sub-thread-Id="20"
context="" token=""] Failed to start repository service. Reason:
System.InvalidOperationException: Configuration section encryptionKey is not
protected
at
DynamicOps.Common.Utils.EncryptionHelpers.ReadKeyFromConfiguration(Configuration
config)
at DynamicOps.Common.Utils.EncryptionHelpers.Decrypt(String value)
at DynamicOps.Repository.Runtime.CoreModel.GlobalPropertyItem.Decrypt(Func`2
decryptFunc)

```

at
DynamicOps.Common.Entity.ContextHelpers.OnObjectMaterializedCallbackEncryptable(Object
t
sender, ObjectMaterializedEventArgs e)
at
System.Data.Common.Internal.Materialization.Shaper.RaiseMaterializedEvents()
at
System.Data.Common.Internal.Materialization.Shaper`1.SimpleEnumerator.MoveNext()
at System.Linq.Enumerable.FirstOrDefault[TSource](IEnumerable`1 source)
at System.Linq.Queryable.FirstOrDefault[TSource](IQueryable`1 source)
at
DynamicOps.Repository.Runtime.Common.GlobalPropertyHelper.GetGlobalPropertyItemValue(CoreModelEntities
coreModelContext, String propertyName, Boolean throwIfPropertyNotFound)
at
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.LoadSolutionUserCertificate()
at
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.InitializeFromDb(String
coreModelConnectionString)
at DynamicOps.Repository.Runtime.Common.RepositoryRuntime.Initialize().

```

Cause

La mise à niveau d'IaaS échoue lorsque la date de création du fichier `web.config` est identique ou ultérieure à la date de modification.

Solution

- 1 Sur l'hôte IaaS, connectez-vous à Windows.
- 2 Ouvrez l'invite de commande Windows.
- 3 Changez les répertoires pour le dossier d'installation de vRealize Automation.
- 4 Démarrez un éditeur de texte avec l'option **Exécuter en tant qu'administrateur**.
- 5 Localisez et sélectionnez le fichier `web.config` et enregistrez le fichier pour modifier sa date de modification.
- 6 Examinez les propriétés du fichier `web.config` afin de confirmer que la date de modification du fichier est postérieure à la date de création.
- 7 Mettez à niveau IaaS.

Manager Service échoue à s'exécuter en raison d'erreurs de validation du certificat SSL pendant l'exécution

Manager Service échoue à s'exécuter en raison d'erreurs de validation du certificat SSL.

Problème

Manager service échoue et renvoie le message d'erreur suivant dans le journal :

```
[Info] : Thread-Id="6" - context="" token="" Échec de la tentative de connexion à la
base de données principale. Nouvelle tentative dans 00:00:05. Détails de l'erreur :
une connexion a été établie avec le serveur, mais une erreur s'est ensuite produite
pendant le processus de connexion. (fournisseur : fournisseur SSL, erreur : 0 - La
chaîne de certificats a été émise par une autorité non autorisée.)
```

Cause

Pendant l'exécution, Manager Service échoue à s'exécuter en raison d'erreurs de validation du certificat SSL.

Solution

- 1 Ouvrez le fichier de configuration `ManagerService.config`.
- 2 Mettez à jour **Encrypt=False** à la ligne suivante :

```
<add name="vcac-repository" providerName="System.Data.SqlClient" connectionString="Data
Source=iaas-db.sqa.local;Initial Catalog=vcac;Integrated Security=True;Pooling=True;Max
Pool Size=200;MultipleActiveResultSets=True;Connect Timeout=200, Encrypt=True" />
```

La connexion échoue après une mise à niveau

Vous devez quitter le navigateur et vous reconnecter après une mise à niveau pour les sessions qui utilisent des comptes d'utilisateurs non synchronisés.

Problème

Après la mise à niveau de vRealize Automation, le système refuse de vous laisser accéder aux comptes d'utilisateurs non synchronisés lors de la connexion.

Solution

Quittez le navigateur et relancez vRealize Automation.

Supprimer les nœuds orphelins sur vRealize Automation

Un nœud orphelin est un nœud dupliqué qui est signalé sur l'hôte mais n'y existe pas.

Problème

Lorsque vous vérifiez que chaque nœud IaaS et dispositif virtuel est sain, vous pouvez découvrir qu'un hôte comporte un ou plusieurs nœuds orphelins. Vous devez supprimer les nœuds orphelins.

Solution

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

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

- 2 Sélectionnez **Cluster**.

- 3 Pour chaque nœud orphelin dans le tableau, cliquez sur **Supprimer**.

La commande Joindre un cluster semble avoir échoué après la mise à niveau d'un environnement à haute disponibilité

Lorsque vous cliquez sur **Joindre un cluster** dans l'interface de gestion du dispositif vRealize Automation sur un nœud de cluster secondaire, l'indicateur de progression disparaît.

Problème

Lorsque vous utilisez l'interface de gestion du dispositif vRealize Automation après une mise à niveau pour joindre un nœud de cluster secondaire au nœud principal, l'indicateur de progression disparaît et aucun message d'erreur ou de réussite ne s'affiche. Ce comportement constitue un problème intermittent.

Cause

L'indicateur de progression disparaît, car certains navigateurs cessent d'attendre une réponse du serveur. Ce comportement n'arrête pas le processus de jonction du cluster. Vous pouvez vérifier que le processus de jonction du cluster est réussi en consultant le fichier journal dans `/var/log/vmware/vcac/vcac-config.log`.

La fusion de la mise à niveau de la base de données PostgreSQL échoue

La fusion de la base de données PostgreSQL externe avec la base de données PostgreSQL intégrée échoue.

Problème

Si la fusion de la mise à niveau de la base de données PostgreSQL échoue, vous pouvez effectuer une fusion manuelle.

Solution

- 1 Rétablissez le dispositif virtuel vRealize Automation sur le snapshot effectué avant la mise à niveau.
- 2 Connectez-vous au dispositif virtuel vRealize Automation et exécutez cette commande pour permettre à la mise à niveau de s'exécuter si la fusion échoue.

```
touch /tmp/allow-external-db
```

La commande ne désactive pas la fusion automatique.

- 3 Sur l'hôte de la base de données PostgreSQL distante, connectez-vous à la base de données PostgreSQL en utilisant l'outil `psql` et exécutez ces commandes.

```
CREATE EXTENSION IF NOT EXISTS "hstore";
```

```
CREATE EXTENSION IF NOT EXISTS "uuid-oss";
```

```
CREATE SCHEMA saas AUTHORIZATION vcac;
```

L'utilisateur dans cette commande est *vcac*. Si vRealize Automation se connecte à la base de données externe avec un utilisateur différent, remplacez *vcac* dans cette commande par le nom de cet utilisateur.

```
CREATE EXTENSION IF NOT EXISTS "citext" SCHEMA saas;
```

- 4 Exécutez la mise à niveau.

Si la mise à niveau réussit, le système fonctionne comme prévu avec la base de données PostgreSQL externe. Vérifiez que la base de données PostgreSQL externe fonctionne correctement.

- 5 Connectez-vous au dispositif virtuel vRealize Automation et exécutez ces commandes

```
/etc/bootstrap/postupdate.d/00-20-db-merge-external
```

```
/etc/bootstrap/postupdate.d/11-db-merge-external
```

La mise à jour du dispositif vRealize Automation de réplica échoue

La mise à jour du dispositif vRealize Automation de réplica échoue pendant la mise à jour du dispositif master.

Cause

La mise à jour d'un dispositif de réplica échoue en raison de problèmes de connectivité ou d'autres problèmes. Dans ce cas, un message d'avertissement s'affiche sur l'onglet **Mise à jour** sur le dispositif vRealize Automation master pour mettre en évidence le réplica dont la mise à jour a échoué.

Solution

- 1 Restaurez le snapshot ou la sauvegarde du dispositif virtuel de réplica jusqu'à l'état antérieur à la mise à jour et mettez-le sous tension.
- 2 Connectez-vous en tant qu'utilisateur racine à l'interface de gestion du dispositif vRealize Automation de réplica.
<https://vrealize-automation-appliance-FQDN:5480>
- 3 Cliquez sur **Mettre à jour > Paramètres**.

- 4 Dans la section Référentiel de mises à jour, choisissez de télécharger les mises à jour depuis un référentiel VMware ou depuis un CD-ROM.
- 5 Cliquez sur **État**.
- 6 Cliquez sur **Vérifier les mises à jour** pour vérifier qu'une mise à jour est accessible.
- 7 Cliquez sur **Installer les mises à jour**.
- 8 Cliquez sur **OK**.

Un message indiquant que la mise à jour est en cours s'affiche.

- 9 Ouvrez les fichiers de journal pour vérifier que la mise à niveau s'effectue correctement.

- /opt/vmware/var/log/vami/vami.log
- /var/log/vmware/horizon/horizon.log

Pendant le processus de mise à niveau, si vous vous déconnectez et que vous vous reconnectez avant la fin de la mise à niveau, vous pouvez continuer de suivre la progression de la mise à jour dans le fichier journal. Le fichier `updatecli.log` peut afficher des informations sur la version de vRealize Automation à partir de laquelle vous effectuez la mise à niveau. Cette version affichée devient la version appropriée plus tard pendant le processus de mise à niveau.

Le temps requis pour terminer la mise à jour dépend de votre environnement.

- 10 Lorsque la mise à jour est terminée, redémarrez le dispositif virtuel.
 - a Cliquez sur **Système**.
 - b Cliquez sur **Redémarrer** et confirmez votre sélection.
- 11 Sélectionnez **Cluster**.
- 12 Entrez le nom de domaine complet du dispositif vRealize Automation master et cliquez sur **Joindre un cluster**.

Copies de sauvegarde de fichiers .xml entraînant l'expiration du délai du système

vRealize Automation enregistre tous les fichiers possédant l'extension .xml dans le répertoire \VMware\VCAC\Server\ExternalWorkflows\xml*. Si ce répertoire contient des fichiers de sauvegarde possédant l'extension .xml, le système exécute les workflows en double qui entraînent l'expiration du délai du système.

Solution : lorsque vous sauvegardez des fichiers dans ce répertoire, déplacez les sauvegardes dans un autre répertoire ou modifiez l'extension .xml dans le nom des fichiers.

Exclure la mise à niveau d'IaaS

Vous pouvez mettre à jour le dispositif vRealize Automation sans mettre à niveau les composants IaaS.

Utilisez la procédure suivante lorsque vous souhaitez mettre à jour le dispositif vRealize Automation sans mettre à niveau les composants IaaS. Cette procédure

- n'arrête pas les services IaaS.
- Ignore la mise à jour des agents de gestion.
- Empêche la mise à jour automatique des composants IaaS après la mise à jour du dispositif vRealize Automation.

Procédure

- 1 Ouvrez une connexion Secure Shell (SSH) au nœud du dispositif vRealize Automation principal.
- 2 À l'invite de commandes, exécutez cette commande pour créer le fichier de basculement :
touch /tmp/disable-iaas-upgrade
- 3 Arrêtez manuellement les services IaaS.
 - a Connectez-vous à votre serveur Windows IaaS.
 - b Sélectionnez **Démarrer > Outils d'administration > Services**.
 - c Arrêtez ces services dans l'ordre suivant.

Note N'arrêtez pas le serveur Windows IaaS.

- 1 Chaque agent proxy VMware vRealize Automation.
 - 2 Chaque VMware DEM Worker.
 - 3 VMware DEM Orchestrator.
 - 4 Le service VMware vCloud Automation Center.
- 4 Accédez à l'interface de gestion du dispositif vRealize Automation et mettez à jour le dispositif vRealize Automation principal.

Impossible de créer un nouveau répertoire dans vRealize Automation

Une tentative d'ajout d'un nouveau répertoire avec le premier connecteur de synchronisation échoue.

Problème

Cette erreur se produit en raison de la présence d'un fichier config-state.json incorrect dans `usr/local/horizon/conf/states/VSPHERE.LOCAL/3001/`.

Pour plus d'informations sur la correction de ce problème, reportez-vous à [l'article 2145438 de la base de connaissances](#).

Expiration du délai de mise à jour du dispositif virtuel de réplica de vRealize Automation

La mise à jour du dispositif virtuel de réplica de vRealize Automation arrive à expiration lors de la mise à jour du dispositif virtuel master.

Problème

Lorsque vous mettez à jour le dispositif virtuel master, l'onglet Mettre à jour de l'interface de gestion du dispositif master vRealize Automation affiche un dispositif virtuel de réplica en surbrillance qui a atteint la limite de délai d'expiration de la mise à jour.

Cause

La mise à jour arrive à expiration en raison d'un problème de performance ou d'infrastructure.

Solution

- 1 Vérifiez l'avancement de la mise à jour du dispositif virtuel de réplica.
 - a Connectez-vous en tant qu'utilisateur racine à l'interface de gestion du dispositif vRealize Automation de réplica.
`https://vrealize-automation-appliance-FQDN:5480`
 - b Sélectionnez **Mettre à jour > État** et vérifiez la progression de la mise à jour.
 Effectuez l'une des opérations suivantes.
 - Si la mise à jour échoue, suivez les étapes décrites dans la rubrique de dépannage [La mise à jour du dispositif vRealize Automation de réplica échoue](#).
 - Si la mise à niveau du dispositif virtuel de réplica est en cours, attendez la fin de la mise à niveau et passez à l'étape 2.
- 2 Redémarrez le dispositif virtuel.
 - a Cliquez sur **Système**.
 - b Cliquez sur **Redémarrer** et confirmez votre sélection.
- 3 Sélectionnez **Cluster**.
- 4 Entrez le nom de domaine complet du dispositif virtuel vRealize Automation master et cliquez sur **Joindre un cluster**.

Aucun déploiement n'est créé pour certaines machines virtuelles cours de la mise à niveau

Les machines virtuelles dont l'état indique qu'elles sont manquantes au moment de la mise à niveau n'ont pas de déploiement correspondant créé dans l'environnement cible.

Problème

Si une machine virtuelle est à l'état « manquant » dans l'environnement source pendant la mise à niveau, aucun déploiement correspondant n'est créé dans l'environnement cible. Si une machine virtuelle sort de l'état manquant après la mise à niveau, vous pouvez importer la machine dans le déploiement cible à l'aide d'une importation en bloc.

Erreur de certificat non approuvé

Lorsque vous affichez la page de la visionneuse du journal de l'infrastructure dans la console dispositif vRealize Automation, vous pouvez voir un rapport d'échec de connexion au point de terminaison avec le message : `Certificate is not trusted`.

Problème

Sur la console dispositif vRealize Automation, sélectionnez **Infrastructure > Surveillance > Journal**. Sur la page de la visionneuse du journal, vous pouvez voir un rapport semblable à celui-ci :

Échec de la connexion au point de terminaison. Pour confirmer que vous pouvez établir une connexion sécurisée à ce point de terminaison, accédez au point de terminaison vSphere sur la page Points de terminaison et cliquez sur le bouton Tester la connexion.

Exception interne : Certificat non approuvé (RemoteCertificateChainErrors). Objet : C=US, CN=vc6.mycompany.com Empreinte : DC5A8816231698F4C9013C42692B0AF93D7E35F1

Cause

La mise à niveau à partir de versions antérieures de vRealize Automation apporte des modifications aux points de terminaison depuis votre environnement d'origine. Après la mise à niveau de vRealize Automation, l'administrateur IaaS doit examiner chaque point de terminaison mis à niveau qui utilise une connexion https sécurisée. Si un point de terminaison renvoie une erreur `Certificate is not trusted`, le point de terminaison ne fonctionne pas correctement.

Solution

- 1 Connectez-vous à la console vRealize Automation en tant qu'administrateur de l'infrastructure.
- 2 Sélectionnez **Infrastructure > Points de terminaison > Points de terminaison**.
- 3 Procédez comme suit pour chaque point de terminaison ayant une connexion sécurisée.
 - a Cliquez sur **Modifier**.
 - b Cliquez sur **Tester la connexion**.
 - c Examinez les détails du certificat et cliquez sur **OK** si vous approuvez ce certificat.
 - d Redémarrez les services Windows pour tous les agents Proxy IaaS utilisés par ce point de terminaison.
- 4 Vérifiez que des erreurs `Certificate is not trusted` ne s'affichent plus sur la page de la visionneuse du journal d'infrastructure.

L'installation de la mise à niveau de vRealize Automation échoue lors de l'application des correctifs requis

L'installation ou la mise à niveau vers vRealize Automation échoue et un message d'erreur figure dans le fichier journal.

Problème

Lorsque vous procédez à l'installation ou à la mise à niveau vers vRealize Automation, la procédure échoue. Cela se produit généralement lorsque l'application d'un correctif au cours de l'installation ou de la mise à niveau échoue. Un message d'erreur figure dans le fichier journal semblable au message suivant : Security error. Applying automatic fix for FIREWALL prerequisite failed. RPM Status 1: Pre install script failed, package test and installation skipped.

Cause

Dans l'environnement Windows, une stratégie de groupe pour l'exécution du script PowerShell est définie sur **Activé**.

Solution

- 1 Sur la machine hôte Windows, exécutez `gpedit.msc` pour ouvrir l'éditeur de stratégie de groupe locale.
- 2 Dans le volet de gauche sous **Configuration ordinateur**, cliquez sur le bouton **Développer** pour ouvrir **Modèles d'administration > Composants Windows > Windows PowerShell**.
- 3 Pour **Activer l'exécution des scripts**, remplacez l'état **Enabled** par **Not Configured**.

Impossible de mettre à jour les composants DEM et DEO

Impossible de mettre à jour les composants DEM et DEO lors de la mise à niveau de vRealize Automation 7.2 vers la version 7.3.x

Problème

Après la mise à niveau de vRealize Automation 7.2 vers la version 7.3.x, les composants DEM et DEO installés sur le chemin d'accès personnalisé, tel que le lecteur D:, ne sont pas mis à jour.

Consultez [l'article 2150517 de la base de connaissances](#).

La mise à jour ne réussit pas à mettre à jour l'agent de gestion

Un message d'erreur sur l'agent de gestion s'affiche lorsque vous cliquez sur **Installer les mises à jour** sur la page d'état de mise à jour de l'interface de gestion du dispositif vRealize Automation.

Problème

Le processus de mise à niveau a échoué. Un message s'affiche : Impossible de mettre à niveau l'agent de gestion sur le nœud x. Parfois ce message mentionne plusieurs nœuds.

Cause

De nombreuses conditions peuvent provoquer ce problème. Le message d'erreur identifie uniquement l'ID du nœud de la machine concernée. Vous trouverez plus d'informations dans le fichier `ALL.log` pour l'agent de gestion sur la machine où la commande a échoué.

Effectuez ces tâches sur les nœuds concernés selon votre situation :

Solution

- ◆ Si le service de l'agent de gestion n'est pas en cours d'exécution, démarrez le service et relancez la mise à niveau sur le dispositif virtuel.
- ◆ Si le service de l'agent de gestion est en cours d'exécution et que l'agent de gestion est mis à niveau, redémarrez la mise à niveau sur le dispositif virtuel.
- ◆ Si le service de l'agent de gestion est en cours d'exécution, mais que l'agent de gestion n'est pas mis à niveau, procédez à une mise à niveau manuelle.
 - a Dans le navigateur, accédez à la page d'installation d'laaS.
`https://vrealize-automation-appliance-FQDN:5480/installer`
 - b Téléchargez et exécutez le programme d'installation de l'agent de gestion.
 - c Redémarrez la machine de l'agent de gestion.
 - d Redémarrez la mise à niveau sur le dispositif virtuel.

La mise à niveau de l'agent de gestion a échoué

La mise à niveau de l'agent de gestion a échoué pendant la mise à niveau de vRealize Automation.

Problème

Si un incident de basculement a permuté l'hôte de l'agent de gestion principal et secondaire, la mise à niveau échoue, car le processus de mise à niveau automatisé ne peut pas trouver l'hôte attendu. Effectuez cette procédure sur chaque nœud laaS sur lequel l'agent de gestion n'est pas mis à niveau.

Solution

- 1 Ouvrez le fichier All.log dans le dossier des journaux de l'agent de gestion, qui se trouve dans `C:\Program Files (x86)\VMware\VCAC\Management Agent\Logs\`.

L'emplacement du dossier d'installation peut être différent de l'emplacement par défaut.

- 2 Recherchez dans le fichier journal un message sur un dispositif virtuel obsolète ou hors tension.

Par exemple, EXCEPTION INTERNE : System.Net.WebException : Impossible de se connecter au serveur distant ----> System.Net.Sockets.SocketException: Une tentative de connexion a échoué, car le participant connecté n'a pas répondu convenablement au-delà d'une certaine durée, ou une connexion établie a échoué car l'hôte de connexion n'a pas répondu `IP_Address:5480`

- 3 Modifiez le fichier de configuration de l'agent de gestion dans C:\Program Files (x86)\VMware\VCAC\Management Agent\VMware.IaaS.Management.Agent.exe.config pour remplacer la valeur alternativeEndpointaddress existante par l'URL du point de terminaison du dispositif virtuel principal.

L'emplacement du dossier d'installation peut être différent de l'emplacement par défaut.

Exemple de valeur alternativeEndpointaddress dans

VMware.IaaS.Management.Agent.exe.config.

```
<alternativeEndpoint address="https://FQDN:5480/" thumbprint="thumbprint number" />
```

- 4 Redémarrez le service de l'agent de gestion Windows et vérifiez le fonctionnement du fichier All.log.

- 5 Exécutez la procédure de mise à niveau sur le dispositif vRealize Automation principal.

Échec de la mise à jour de vRealize Automation en raison des paramètres de délai d'expiration par défaut

Vous pouvez augmenter le paramètre de temporisation pour la mise à jour si le paramètre par défaut pour la synchronisation des bases de données est trop court pour votre environnement.

Problème

Le paramètre de délai d'expiration pour la commande Vcac-Config SynchronizeDatabases n'est pas suffisant pour certains environnements où la synchronisation des bases de données est plus longue que la valeur par défaut de 3 600 secondes.

Les valeurs des propriétés cafeTimeoutInSeconds et cafeRequestPageSize dans le fichier Vcac-Config.exe.config régissent la communication entre l'API et l'utilitaire Vcac-config.exe. Le fichier se trouve à *l'emplacement d'installation d'IaaS\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe.config*.

Vous pouvez remplacer la valeur de délai d'expiration par défaut uniquement pour la commande SynchronizeDatabases en fournissant une valeur pour ces paramètres facultatifs.

Paramètre	Nom court	Description
--DatabaseSyncTimeout	-dstm	Définit la valeur de délai d'expiration de demande HTTP uniquement pour SynchronizeDatabases en secondes.
--DatabaseSyncPageSize	-dsps	Définit la taille de page de demande de synchronisation uniquement pour la synchronisation de réservation ou de stratégie de réservation. La valeur par défaut est 10.

Si ces paramètres ne sont pas définis dans le fichier Vcac-Config.exe.config, le système utilise le délai d'expiration par défaut.

Échec de la mise à niveau d'laaS dans un environnement haute disponibilité

Échec du processus de mise à niveau d'laaS sur le nœud du serveur Web principal sur lequel l'équilibrage de charge est activé. Vous pouvez voir ces messages d'erreur :

« System.Net.WebException : L'opération a expiré » ou « 401 - Non autorisé : L'accès est refusé en raison d'informations d'identification non valides. »

Problème

La mise à niveau d'laaS lorsque l'équilibrage de charge est activé peut provoquer un échec intermittent. Dans ce cas, vous devez réexécuter la mise à niveau de vRealize Automation en désactivant l'équilibrage de charge au préalable.

Solution

- 1 Restaurez votre environnement aux snapshots antérieurs à la mise à jour.
- 2 Ouvrez une connexion Bureau à distance au nœud de serveur Web laaS principal.
- 3 Accédez au fichier d'hôtes Windows dans c:\windows\system32\drivers\etc.
- 4 Ouvrez le fichier d'hôtes et ajoutez cette ligne pour qu'il contourne l'équilibrage de charge du serveur Web.

IP_address_of_primary_iaas_website_node vrealizeautomation_iaas_website_lb_fqdn

Exemple :

10.10.10.5 vra-iaas-web-lb.domain.com

- 5 Enregistrez le fichier d'hôtes et réessayez la mise à jour de vRealize Automation.
- 6 À la fin de la mise à jour de vRealize Automation, ouvrez le fichier d'hôtes et supprimez la ligne que vous avez ajoutée à l'étape 4.

Les stockages peuvent être différés après la mise à niveau

Les stockages ne s'affichent pas sous l'onglet Réserveation.

Si les stockages ne s'affichent pas dans l'onglet Réservations après la mise à niveau, un redémarrage de vcac-server est requis sur tous les nœuds. L'affichage des stockages peut prendre jusqu'à une heure dans la section des ressources sous l'onglet Réservations.

Résoudre les problèmes de mise à niveau

Vous pouvez modifier le processus de mise à niveau pour résoudre les problèmes associés.

Lorsque vous rencontrez des problèmes de mise à niveau de votre environnement vRealize Automation, utilisez cette procédure pour modifier le processus de mise à niveau en sélectionnant l'un des indicateurs disponibles.

Solution

- 1 Ouvrez une connexion Secure Shell (SSH) au nœud du dispositif vRealize Automation principal.

- 2 À l'invite de commandes, exécutez cette commande pour créer le fichier de basculement :

touch *available_flag*

Par exemple : **touch /tmp/disable-iaas-upgrade**

Tableau 1-58. Indicateurs disponibles

Indicateur	Description
/tmp/disable-iaas-upgrade	<ul style="list-style-type: none"> ■ Empêche le processus de mise à niveau d'IaaS après le redémarrage du dispositif virtuel. ■ Empêche la mise à niveau de l'agent de gestion. ■ Empêche les vérifications et les correctifs automatiques de conditions préalables. ■ Empêche l'arrêt des services IaaS.
/tmp/do-not-upgrade-ma	Empêche la mise à niveau de l'agent de gestion. Cet indicateur est approprié lorsque l'agent de gestion est mis à niveau manuellement.
/tmp/skip-prereq-checks	Empêche les vérifications et les correctifs automatiques de conditions préalables. Cet indicateur est approprié lorsqu'il existe un problème lié aux correctifs automatiques de conditions préalables et que ceux-ci ont dû être appliqués manuellement.
/tmp/do-not-stop-services	Empêche l'arrêt des services IaaS. La mise à niveau n'arrête pas les services Windows IaaS tels que le service de gestion, les DEM et les agents.
/tmp/do-not-upgrade-servers	<p>Empêche la mise à niveau automatique de tous les composants Server IaaS tels que la base de données, le site Web, WAPI, le référentiel, les données de modèle Mfrontanager et le service de gestion.</p> <p>Note Cet indicateur empêche également l'activation du mode de basculement automatique du service de gestion.</p>
/tmp/do-not-upgrade-dems	Empêche la mise à niveau de DEM.
/tmp/do-not-upgrade-agents	Empêche la mise à niveau de l'agent proxy IaaS.

3 Effectuez les tâches correspondant à l'indicateur choisi.

Tableau 1-59. Tâches supplémentaires

Indicateur	Tâches
/tmp/disable-iaas-upgrade	<ul style="list-style-type: none"> ■ Mettez à niveau manuellement l'agent de gestion. ■ Appliquez manuellement toutes les conditions préalables IaaS requises. ■ Arrêtez manuellement les services IaaS. <ol style="list-style-type: none"> a Connectez-vous à votre serveur Windows IaaS. b Sélectionnez Démarrer > Outils d'administration > Services. c Arrêtez ces services dans l'ordre suivant. <p>Note N'arrêtez pas le serveur Windows IaaS.</p> <ol style="list-style-type: none"> a Chaque agent proxy VMwarevRealize Automation. b Chaque VMware DEM Worker. c VMware DEM Orchestrator. d Le service VMware vCloud Automation Center. ■ Démarrez manuellement la mise à niveau d'IaaS après celle du dispositif virtuel.
/tmp/do-not-upgrade-ma	Mettez à niveau manuellement l'agent de gestion.
/tmp/skip-prereq-checks	Appliquez manuellement toutes les conditions préalables IaaS requises.
/tmp/do-not-stop-services	<p>Arrêtez manuellement les services IaaS.</p> <ol style="list-style-type: none"> 1 Connectez-vous à votre serveur Windows IaaS. 2 Sélectionnez Démarrer > Outils d'administration > Services. 3 Arrêtez ces services dans l'ordre suivant. <p>Note N'arrêtez pas le serveur Windows IaaS.</p> <ol style="list-style-type: none"> a Chaque agent proxy VMwarevRealize Automation. b Chaque VMware DEM Worker. c VMware DEM Orchestrator. d Le service VMware vCloud Automation Center.
/tmp/do-not-upgrade-servers	
/tmp/do-not-upgrade-dems	
/tmp/do-not-upgrade-agents	

- 4 Accédez à la console de gestion du dispositif vRealize Automation et mettez à jour le dispositif vRealize Automation principal.

Note Étant donné que chaque indicateur reste actif jusqu'à ce qu'il soit supprimé, exécutez cette commande pour supprimer l'indicateur choisi après la mise à niveau :

rm /*flag_path*/*flag_name*. Par exemple, **rm /tmp/disable-iaas-upgrade.**

Échec de la mise à niveau du dispositif virtuel lors de la vérification des conditions préalables IaaS

La vérification des conditions préalables IaaS ne parvient pas à valider les environnements configurés avec un nom de site Web IIS personnalisé. La désactivation de la mise à niveau d'IaaS automatisée corrige le problème.

Problème

La mise à niveau du dispositif virtuel échoue lors de la vérification des conditions préalables IaaS lors de l'exécution de scripts de préinstallation et de scripts de post-installation.

Error: Unrecognized configuration path MACHINE/WEBROOT/APPHOST/Default Web Site can not find path IIS:\Sites\Default Web Site because it does not exist.

Lorsque l'échec se produit, un message d'erreur similaire au message suivant s'affiche : Applying automatic fix for <*prerequisite check name*> prerequisite failed.

Cause

L'outil de vérification des conditions préalables IaaS ne parvient pas à valider les environnements configurés avec un nom de site Web IIS personnalisé. Pour corriger le problème, vous devez désactiver l'outil de vérification des conditions préalables automatisées d'IaaS.

Solution

- 1 Désactivez les vérifications et correctifs des conditions préalables automatisées de mise à niveau d'IaaS.
- 2 Procédez à la mise à niveau de vRealize Automation. Consultez [Résoudre les problèmes de mise à niveau](#).
- 3 Suivez les invites de mise à niveau. Lorsque les invites vous dirigent à redémarrer vRealize Automation, vous pouvez utiliser le programme d'installation d'IaaS pour rechercher les conditions préalables IaaS non satisfaites et les corriger manuellement.

Note Ne redémarrez pas le dispositif tant que vous n'avez pas terminé la validation des conditions préalables IaaS.

- 4 Utilisez les étapes suivantes pour chaque nœud de site Web IaaS.
 - a Téléchargez le programme d'installation d'IaaS. Consultez [Télécharger le programme d'installation d'IaaS pour mettre à niveau les composants IaaS après la mise à niveau du dispositif vRealize Automation](#).

- b La première fois que vous initialisez le programme d'installation d'laaS, il génère un nouveau fichier de configuration sous le même répertoire avec l'extension `.exe.config`.
 - c Fermez le programme d'installation d'laaS et ajoutez la clé suivante dans la section `<appSettings>` du fichier de configuration. La clé transmet le nom de votre site Web personnalisé à l'outil de vérification des conditions préalables laaS.


```
<add key="PreReqChecker.Default.DefaultWebSite" value="custom_web_site_name"/>
```
 - d Enregistrez le fichier de configuration et relancez le programme d'installation d'laaS. Suivez les instructions à l'écran, jusqu'à ce que la validation des conditions préalables soit terminée. Si des conditions préalables ont été importées, corrigez-les manuellement.
- 5 Activez la mise à niveau automatique d'laaS en fermant le programme d'installation d'laaS et en redémarrant le dispositif vRealize Automation mis à niveau.

Note Si vous décidez de continuer manuellement la mise à niveau d'laaS à l'aide du programme d'installation d'laaS, redémarrez d'abord le dispositif vRealize Automation mis à niveau et attendez que tous les services soient enregistrés. Il vous faut mettre à niveau et configurer tous les systèmes qui possèdent des composants laaS. Pour plus d'informations, reportez-vous à la section [Mettre à niveau les composants laaS après la mise à niveau de vRealize Automation vers la version cible](#).

Mise à niveau de vRealize Automation 6.2.5 vers la version 7.5

Lorsque vous mettez à niveau votre environnement vRealize Automation 6.2.5 vers la version 7.5, vous utilisez des procédures de mise à niveau spécifiques à l'environnement 6.2.5.

Ces informations sont spécifiques à la mise à niveau de vRealize Automation 6.2.5 vers la version 7.5. Pour obtenir des informations sur les autres chemins de mise à niveau pris en charge, reportez-vous à la section [Mise à niveau et migration de vRealize Automation](#).

Mise à niveau depuis vRealize Automation 6.2.5

Vous pouvez effectuer une mise à niveau sur place de votre environnement vRealize Automation 6.2.5 actuel. Vous utilisez les procédures de mise à niveau spécifiques de cette version pour mettre à niveau votre environnement.

Une mise à niveau sur place est un processus en trois étapes. Vous mettez à jour les composants de votre environnement actuel dans l'ordre suivant.

- 1 Dispositif vRealize Automation
- 2 Serveur Web laaS
- 3 Migrer vRealize Orchestrator

Vous devez mettre à niveau tous les composants du produit vers la même version.

L'outil assistant de mise à jour de test de production vRealize analyse votre environnement vRealize Automation 6.2.x, recherche les configurations de fonctionnalités qui peuvent entraîner des problèmes de mise à niveau et vérifie que votre environnement est prêt pour la mise à niveau. Pour télécharger cet outil et la documentation associée, accédez à la page de téléchargement du produit [Outil de test de production VMware vRealize](#).

Les contrôles du dictionnaire de propriétés qui ne sont pas pris en charge après la mise à niveau peuvent être restaurés à l'aide de vRealize Orchestrator et de relations de dictionnaire de propriétés.

Si des workflows dans votre environnement source contiennent du code obsolète, reportez-vous à [vRealize Automation Extensibility Migration Guide](#) pour obtenir des informations sur les modifications du code requises pour la conversion en abonnements aux événements du broker.

À partir de vRealize Automation 7.2, JFrog Artifactory Pro n'est plus inclus dans le dispositif vRealize Automation. Si vous procédez à une mise à niveau d'une version antérieure de vRealize Automation, le processus de mise à niveau supprime JFrog Artifactory Pro. Pour plus d'informations, reportez-vous à [l'article 2147237 de la base de connaissances](#).

Note Si vous avez personnalisé votre environnement vRealize Automation 6.2.5 actuel, contactez l'équipe d'assistance pour obtenir des informations supplémentaires sur la mise à niveau.

Conditions préalables pour la mise à niveau de vRealize Automation

Avant d'effectuer la mise à niveau à partir de vRealize Automation 6.2.5, passez en revue les conditions préalables suivantes.

Conditions requises de la configuration système

Assurez-vous que la configuration système requise suivante est respectée avant de commencer la mise à niveau.

- Vérifiez que tous les dispositifs et serveurs faisant partie de votre déploiement respectent la configuration système requise pour la dernière version. Reportez-vous au vRealize Automation lien vers la matrice de support dans la [documentation du produit vRealize Automation](#).
- Consultez la *Matrice d'interopérabilité des produits VMware* sur le site Web VMware pour obtenir des informations sur la compatibilité avec d'autres produits VMware. Reportez-vous au vRealize Automation lien vers les matrices d'interopérabilité dans la [documentation du produit vRealize Automation](#).
- Vérifiez que l'instance de vRealize Automation que vous mettez à niveau se trouve dans une condition de fonctionnement stable. Corrigez tous les problèmes avant la mise à niveau.
- Si vous procédez à la mise à niveau de vRealize Automation 6.2.5, enregistrez la clé de licence vCloud Suite que vous utilisez pour votre environnement vRealize Automation actuel. Lors de la mise à niveau, les clés de licence existantes sont supprimées de la base de données.

- Assurez-vous d'avoir modifié les paramètres du délai d'expiration d'équilibrage de charge de la valeur par défaut à au moins 10 minutes.

Configuration matérielle requise

Vérifiez que le matériel de votre environnement est adapté à votre version de vRealize Automation cible.

Reportez-vous à [Spécifications matérielles et capacité maximale de vRealize Automation](#)

Assurez-vous que la configuration système requise suivante est respectée avant de commencer la mise à niveau.

- Vous devez configurer votre matériel actuel avant de télécharger la mise à niveau. Reportez-vous à [Augmenter les ressources matérielles de vCenter Server pour vRealize Automation 6.2.5](#).

- Avant de procéder à la mise à niveau, vous devez au moins disposer de la configuration suivante : 18 Go de RAM, 4 CPU, Disque1 = 50 Go, Disque3 = 25 Go et Disque4 = 50 Go.

Si la machine virtuelle est sur vCloud Networking and Security, vous devrez éventuellement allouer plus d'espace RAM.

Bien que vCloud Networking and Security ne bénéficie plus du support technique, les propriétés personnalisées de VCNS restent valides pour NSX. Consultez l'[article 2144733 de la base de connaissances](#).

- Ces nœuds doivent disposer d'au moins 5 Go d'espace disque libre :
 - Site Web IaaS principal
 - Base de données Microsoft SQL
 - Model Manager
- Pour télécharger et exécuter la mise à niveau, vous devez disposer des ressources suivantes :
 - Au moins 15 Go sur la partition racine
 - 5 Go sur la partition /storage/db pour dispositif vRealize Automation master
 - 15 Go sur la partition racine pour chaque dispositif virtuel de réplica
- Vérifiez le sous-dossier /storage/log et supprimez les anciens fichiers ZIP archivés pour libérer de l'espace.

Conditions préalables générales

Assurez-vous que la configuration système requise suivante est respectée avant de commencer la mise à niveau.

- Sauvegardez le fichier `setenv.sh` avant de démarrer la mise à niveau, car les mises à jour personnalisées de ce fichier sont remplacées après la mise à niveau. Le fichier se trouve dans `/usr/lib/vco/app-server/bin/setenv.sh`. Mettez à jour les valeurs au moment approprié après la mise à niveau et redémarrez `vco-server` pour appliquer les modifications.

- Vous disposez d'un accès à un compte Active Directory au format nomutilisateur@domaine et des autorisations pour lier l'annuaire.
- Les conditions suivantes sont respectées :
 - Vous avez accès à un compte avec un format SAMaccountName.
 - Vous disposez de privilèges suffisants pour joindre le système au domaine en créant de façon dynamique un objet ordinateur ou pour le faire fusionner avec un objet créé au préalable.
- Vous avez accès à toutes les bases de données et à tous les équilibres de charge affectés par ou participant à la mise à niveau de vRealize Automation.
- Vous rendez le système indisponible pour les utilisateurs pendant que vous effectuez la mise à niveau.
- Vous désactivez les applications qui interrogent vRealize Automation.
- Vérifiez que le coordinateur de transaction distribué Microsoft (MS DTC) est activé sur tous les serveurs vRealize Automation et SQL associés. Pour des instructions, consultez [l'article 2089503 de la base de connaissances](#).
- Si votre environnement dispose d'un dispositif vRealize Orchestrator externe et d'un dispositif vRealize Orchestrator externe connecté au dispositif Identity Appliance, mettez à niveau vRealize Orchestrator avant de mettre à niveau vRealize Automation.
- Vous devez effectuer des tâches supplémentaires pour préparer vos machines virtuelles vRealize Automation avant de procéder à la mise à niveau. Avant de procéder à la mise à niveau, consultez [l'article 51531 de la base de connaissances](#).
- Assurez-vous d'avoir modifié les paramètres du délai d'expiration d'équilibrage de charge de la valeur par défaut à au moins 10 minutes.
- Si vous utilisez le plug-in DynamicTypes, exportez la configuration du plug-in DynamicTypes vRealize Orchestrator en tant que module.
 - a Connectez-vous à Java Client en tant qu'utilisateur administrateur.
 - b Sélectionnez l'onglet **Workflows**.
 - c Sélectionnez **Bibliothèque > Types dynamiques > Configuration**.
 - d Sélectionnez le workflow Exporter la configuration en tant que module et exécutez-le.
 - e Cliquez sur **Non définie > Insérer valeur**.
 - f Sélectionnez les espaces de noms à exporter et cliquez sur **Ajouter** pour les ajouter au module.
 - g Cliquez sur **Envoyer** pour exporter le module.

- Suivez ces étapes si vous mettez à niveau un environnement distribué configuré avec une base de données PostgreSQL intégrée.
 - a Examinez les fichiers dans le répertoire pgdata sur l'hôte master avant de mettre à niveau les hôtes de réplica.
 - b Accédez au dossier de données PostgreSQL sur l'hôte master dans `/var/vmware/vpostgres/current/pgdata/`.
 - c Fermez et supprimez tous les fichiers .swp dans le répertoire pgdata. Les fichiers portant le suffixe .swp vous obligent à fermer la session VI et à supprimer le fichier.
 - d Vérifiez que tous les fichiers contenus dans ce répertoire ont le nom du propriétaire adéquat : `postgres:<owner-group>`.

Remarques relatives à la mise à niveau vers cette version de vRealize Automation

vRealize Automation 7 et versions ultérieures introduit diverses modifications fonctionnelles pendant et après la mise à niveau. Vous devez vérifier les modifications avant de mettre à niveau votre déploiement vRealize Automation 6.2.5 vers la nouvelle version.

Vérifiez ces éléments à prendre en compte avant de procéder à la mise à niveau.

Mise à niveau et spécifications Identity Appliance

Pendant le processus de mise à niveau de vRealize Automation, vous répondez à des invites pour mettre à niveau le dispositif Identity Appliance.

Le déploiement cible utilise VMware Identity Manager.

Mise à niveau et attribution de licence

Lors de la mise à niveau, vos licences vRealize Automation 6.2.5 existantes et toutes les licences vCloud Suite 6.x dont vous disposez sont supprimées. Vous devez saisir à nouveau vos licences dans l'interface de gestion du dispositif vRealize Automation de la version de vRealize Automation cible.

L'attribution de licence vRealize Automation pour les dispositifs virtuels et IaaS s'effectue désormais en entrant les informations de clé de licence dans le dispositif vRealize Automation. Les informations de licence ne sont plus disponibles dans l'interface utilisateur IaaS et IaaS n'effectue plus de contrôle de licence. Les points de terminaison et les quotas sont appliqués dans le cadre des contrats de licence d'utilisateur final.

Note Notez votre clé de licence vCloud Suite 6.x si vous l'avez utilisée pour vRealize Automation 6.2.5 avant la mise à niveau. Lors de la mise à niveau, les clés de licence existantes sont supprimées de la base de données.

Pour plus d'informations concernant la nouvelle saisie de vos informations relatives à la licence pendant ou après la mise à niveau, consultez [Mettre à jour la clé de licence](#).

Présentation de la mise à niveau des rôles

Lorsque vous mettez à niveau vRealize Automation, les attributions de rôles existants de votre organisation sont conservées. La mise à niveau crée également des attributions de rôles afin de prendre en charge des rôles d'architecte de Blueprint supplémentaires.

Les rôles d'architecte suivants sont utilisés pour prendre en charge la définition du Blueprint dans le canevas de conception :

- Architecte d'application. Assemble des composants et Blueprints existants pour créer des Blueprints composites.
- Architecte d'infrastructure. Crée et gère des Blueprints de machine virtuelle.
- Architecte XaaS. Créer et gère des Blueprints XaaS.
- Architecte de logiciel. Crée et gère des composants Logiciel.

Dans vRealize Automation 7, les administrateurs de locataires et les gestionnaires de groupes d'activités ne peuvent pas concevoir de Blueprints par défaut. Les administrateurs de locataires et les gestionnaires de groupes d'activités mis à niveau se voient attribuer le rôle d'architecte d'infrastructure.

Les utilisateurs qui peuvent reconfigurer une machine virtuelle dans la version source de vRealize Automation 6.2.x peuvent modifier la propriété de la machine virtuelle après la mise à niveau vers la nouvelle version.

Les attributions de rôle suivantes sont effectuées au cours de la mise à niveau. Les rôles qui ne sont pas répertoriés dans le tableau sont mis à niveau vers le même nom de rôle dans le déploiement cible.

Tableau 1-60. Rôles attribués lors de la mise à niveau

Rôle dans le déploiement source	Rôle dans le déploiement cible
Administrateur de locataire	Administrateur de locataire et architecte d'infrastructure
Gestionnaire de groupes d'activité	Gestionnaire de groupe d'activité et architecte d'infrastructure
Architecte de services	Architecte XaaS
Architecte d'application	Architecte de logiciel

Pour plus d'informations sur les rôles, reportez-vous à [Rôles et responsabilités des locataires dans vRealize Automation](#).

Présentation de la mise à niveau des Blueprints

En règle générale, les Blueprints publiés sont mis à niveau en tant que Blueprints publiés.

Cependant, cette règle comporte quelques exceptions. Les Blueprints avec plusieurs machines sont mis à niveau en tant que Blueprints composites contenant des composants de Blueprint. Les Blueprints avec plusieurs machines qui contiennent des paramètres non pris en charge sont mis à niveau en tant qu'éléments non publiés.

Note vRealize Automation 7.x prend un snapshot de Blueprint au moment du déploiement. Si vous rencontrez des problèmes de reconfiguration lors de la mise à jour des propriétés de la machine telles que le CPU et la RAM de la machine dans un déploiement, consultez l'article de la base de connaissances [2150829 vRA 7.x Blueprint Snapshotting](#).

Pour plus d'informations sur la mise à niveau des Blueprints, reportez-vous aux sections [Mise à niveau et Blueprints de vApp, points de terminaison vCloud et réservations vCloud](#) et [Présentation de la mise à niveau des Blueprints avec plusieurs machines](#).

Mise à niveau et Blueprints de vApp, points de terminaison vCloud et réservations vCloud

Vous ne pouvez pas mettre à niveau un déploiement qui contient des points de terminaison vApp (vCloud). La présence de points de terminaison vApp (vCloud) empêche la mise à niveau vers cette version vRealize Automation.

La mise à niveau échoue sur le dispositif virtuel master s'il existe un point de terminaison vApp (vCloud) dans le déploiement source. Un message s'affiche dans l'interface utilisateur et le journal. Pour déterminer si votre déploiement source contient un point de terminaison vApp (vCloud), connectez-vous à la console vRealize Automation en tant qu'utilisateur d'administrateur IaaS. Sélectionnez **Infrastructure > Points de terminaison**. Si la liste des points de terminaison contient des points de terminaison vApp (vCloud), vous ne pouvez pas effectuer la mise à niveau vers cette version vRealize Automation.

Les vApp gérés pour vCloud Air ou les ressources vCloud Director ne sont pas prises en charge dans l'environnement vRealize Automation cible.

Note Les types de stratégie d'approbation suivants sont déconseillés. S'ils figurent dans la liste des types de stratégie d'approbation disponibles après la mise à niveau, ils sont inutilisables.

- Catalogue de services - Demande d'élément de catalogue - vApp
 - Catalogue de services - Demande d'élément de catalogue - Composant vApp
-

Vous pouvez créer des points de terminaison et des réservations vCloud Air et vCloud Director dans le déploiement cible. Vous pouvez également créer des Blueprints avec des composants de machine virtuelle vCloud Air ou vCloud Director.

Présentation de la mise à niveau des Blueprints avec plusieurs machines

Vous pouvez mettre à niveau des Blueprints multi-machine de service géré depuis un déploiement pris en charge de vRealize Automation 6.2.x.

Lorsque vous mettez à niveau un Blueprint avec plusieurs machines, les Blueprints de composant sont mis à niveau en tant que Blueprints de machine unique séparés. Le Blueprint avec plusieurs machines est mis à niveau en tant que Blueprint composite dans lequel ses Blueprints enfants sont imbriqués sous forme de composants de Blueprint séparés.

La mise à niveau crée un Blueprint composite unique dans le déploiement cible contenant un composant de machine virtuelle par Blueprint de composant dans le Blueprint source avec plusieurs machines. Si un Blueprint a un paramètre qui n'est pas pris en charge dans la nouvelle version, le Blueprint est mis à niveau et défini sur l'état de brouillon. Par exemple, si le Blueprint avec plusieurs machines contient un profil de réseau privé, la mise à niveau ignore le paramètre de profil et le Blueprint est mis à niveau à l'état de brouillon. Vous pouvez modifier le brouillon de Blueprint pour entrer les informations de profil réseau prises en charge et les publier.

Note Si un Blueprint publié dans le déploiement source est mis à niveau vers un Blueprint d'état non publié, il ne fait plus partie d'un service ou d'un droit d'accès. Après avoir mis à niveau et publié le Blueprint dans la version vRealize Automation mise à niveau, vous devez recréer ses stratégies d'approbation ou droits d'accès nécessaires.

Certains réglages de Blueprint avec plusieurs machines ne sont pas pris en charge dans le déploiement vRealize Automation cible, y compris des profils de réseau privés et de réseau routé avec des paramètres PLR Edge. Si vous avez utilisé une propriété personnalisée pour spécifier les paramètres PLR Edge (`VCNS.LoadBalancerEdgePool.Names`), la propriété personnalisée est mise à niveau.

Vous pouvez mettre à niveau un Blueprint avec plusieurs machines avec des points de terminaison vSphere et des paramètres réseau et de sécurité NSX. Le Blueprint mis à niveau contient des composants réseau et de sécurité NSX dans le canevas de conception.

Note Les spécifications de passerelle routée pour les Blueprints avec plusieurs machines, définies dans les réservations, sont mises à niveau. En revanche, le déploiement cible de vRealize Automation ne prend pas en charge les réservations pour les profils routés contenant des paramètres PLR Edge associés. Si la réservation source contient une valeur de passerelle routée pour un PLR Edge, la réservation est mise à niveau, mais le paramètre de la passerelle routée est ignoré. Par conséquent, la mise à niveau génère un message d'erreur dans le fichier journal et la réservation est désactivée.

Lors de la mise à niveau, les espaces et les caractères spéciaux sont supprimés des noms de composants réseau et de sécurité référencés.

Note vRealize Automation 7.x prend un snapshot de Blueprint au moment du déploiement. Si vous rencontrez des problèmes de reconfiguration lors de la mise à jour des propriétés de la machine telles que le CPU et la RAM de la machine dans un déploiement, consultez l'article de la base de connaissances [2150829 vRA 7.x Blueprint Snapshotting](#).

En fonction du type de paramètre, les informations réseau et de sécurité sont capturées comme plusieurs paramètres différents dans le nouveau Blueprint.

- Paramètres pour le Blueprint global sur sa page de propriétés. Ces informations incluent l'isolation d'application, la zone de transport et la passerelle routée ou la stratégie de réservation NSX Edge.

- Paramètres disponibles pour les composants de machine virtuelle vSphere dans les composants réseau et de sécurité NSX dans le canevas de conception.
- Paramètres dans les onglets réseau et sécurité des composants individuels de machine virtuelle vSphere dans le canevas de conception.

Mise à niveau et points de terminaison, réservations et Blueprints physiques

Vous ne pouvez pas mettre à niveau un déploiement qui contient des points de terminaison physiques. S'il existe des points de terminaison physiques, le processus de mise à niveau de vRealize Automation échoue.

La mise à niveau échoue sur le dispositif virtuel master lorsque le déploiement de vRealize Automation 6.2.x dispose d'un point de terminaison physique. Un message d'erreur s'affiche dans l'interface de migration et le journal. Pour déterminer si votre déploiement de vRealize Automation 6.2.x dispose d'un point de terminaison physique, connectez-vous à vRealize Automation en tant qu'utilisateur administrateur laaS. Sélectionnez **Infrastructure > Points de terminaison**, puis passez en revue la liste des points de terminaison. Si la liste comporte un point de terminaison Platform Type Physical, vous ne pouvez pas effectuer de mise à niveau vers vRealize Automation 7.0 et versions ultérieures.

Les points de terminaison physiques, les réservations et les composants de machine virtuelle dans les Blueprints ne sont pas pris en charge par vRealize Automation 7.0 et versions ultérieures.

Mise à niveau et paramètres de profil réseau

Les profils de réseau privé ne sont pas pris en charge par vRealize Automation 7 et versions ultérieures. Ces profils sont ignorés lors de la mise à niveau. Les profils de réseau routés avec paramètres PLR Edge associés ne sont pas non plus pris en charge dans vRealize Automation 7 et versions ultérieures. Ces profils sont également ignorés lors de la mise à niveau.

Le type de profil de réseau privé n'est pas pris en charge dans vRealize Automation 7 et versions ultérieures. Lorsque le processus de mise à niveau de vRealize Automation trouve un profil de réseau privé dans le déploiement source, il l'ignore. Les équilibrages de charge faisant référence à ces réseaux privés sont également ignorés lors de la mise à niveau. Les mêmes conditions de mise à niveau sont applicables pour un profil de réseau routé auquel des paramètres PLR Edge sont associés. Aucune configuration de profil réseau n'est mise à niveau.

Si une réservation contient un profil de réseau privé, les paramètres du profil de réseau privé sont ignorés pendant la mise à niveau. La réservation est mise à niveau comme étant désactivée dans le déploiement cible.

Si une réservation contient un profil de réseau routé avec des paramètres PLR Edge associés, la spécification du profil de réseau routé est ignorée pendant la mise à niveau. La réservation est mise à niveau comme étant désactivée dans le déploiement cible.

Pour obtenir des informations relatives à la mise à niveau d'un Blueprint avec plusieurs machines contenant des réglages réseau, consultez [Présentation de la mise à niveau des Blueprints avec plusieurs machines](#).

Mise à niveau et actions autorisées

Vous ne pouvez pas mettre à niveau les actions d'une machine virtuelle.

Les actions que vous pouvez réaliser sur les machines virtuelles provisionnées, en fonction des spécifications de Blueprint, ne sont pas mises à niveau. Pour recréer les actions que vous pouvez effectuer sur une machine virtuelle, personnalisez les droits pour les Blueprints afin d'activer uniquement certaines actions.

Pour des informations complémentaires, reportez-vous à [Actions dans les droits](#).

Mise à niveau et propriétés personnalisées

Toutes les propriétés personnalisées fournies par vRealize Automation sont disponibles dans le déploiement mis à niveau. Les propriétés personnalisées et les groupes de propriétés sont mis à niveau.

Terminologie et modifications connexes

Tous les profils de la version que vous créez dans le déploiement source sont mis à niveau comme groupes de propriétés. Le terme *profil de déploiement* a été supprimé.

Le terme *jeu de propriétés* a été supprimé et les fichiers de jeu de propriétés CSV ne sont plus disponibles.

Sensibilité à la casse dans les noms des propriétés personnalisées

Avant vRealize Automation 7.0, les noms des propriétés personnalisées n'étaient pas sensibles à la casse. Dans vRealize Automation 7.0 et versions ultérieures, les noms des propriétés personnalisées sont sensibles à la casse. Pendant la mise à niveau, les noms des propriétés personnalisées doivent correspondre exactement. Cela garantit que les valeurs de propriété ne se remplaceront pas mutuellement et qu'elles correspondent aux définitions du dictionnaire de propriétés. Par exemple, une propriété personnalisée `hostname` et une autre propriété personnalisée `HOSTNAME` sont considérés comme des propriétés personnalisées différentes par vRealize Automation 7.0 et versions ultérieures. La propriété personnalisée `hostname` et la propriété personnalisée `HOSTNAME` ne se remplacent pas mutuellement pendant la mise à niveau.

Espaces dans les noms de propriétés personnalisées

Avant la mise à niveau vers cette version de vRealize Automation, supprimez tous les caractères d'espace de vos noms de propriétés personnalisées, par exemple remplacez l'espace par le caractère underscore, afin de permettre à la propriété personnalisée d'être reconnue dans l'installation mise à jour de vRealize Automation. Les noms des propriétés personnalisées vRealize Automation ne peuvent pas contenir d'espaces. Ce problème peut également avoir une incidence sur l'utilisation d'une installation vRealize Orchestrator mise à niveau qui utilise des propriétés personnalisées qui contenaient des espaces dans les versions antérieures de vRealize Automation, de vRealize Orchestrator ou des deux.

Noms de propriété réservés

Plusieurs mots-clés sont désormais réservés. Cela peut donc avoir une incidence sur certaines propriétés mises à niveau. Certains mots-clés utilisés par le code de Blueprint peuvent être importés, par exemple, en utilisant les fonctions d'importation de Blueprint vRealize CloudClient. Ces mots-clés sont considérés comme réservés et ne sont pas disponibles pour les propriétés mises à niveau. Les mots-clés peuvent inclure, sans s'y limiter, `cpustorage` et `memory`.

Mise à niveau et Application Services

Après la migration vers la version de vRealize Automation cible, vous pouvez utiliser l'outil de migration de vRealize Automation Application Services pour mettre à niveau les services d'application.

Suivez ces étapes pour télécharger l'outil.

- 1 Cliquez sur [Télécharger VMware vRealize Automation](#).
- 2 Sélectionnez **Pilotes et outils > VMware vRealize Application Services Migration Tool**.

Mise à niveau et Advanced Service Design

Lorsque vous réalisez une mise à niveau vers vRealize Automation 7 et versions ultérieures, vos éléments de conception des services avancés sont mis à niveau vers des éléments XaaS.

Les composants XaaS sont disponibles pour une utilisation dans le canevas de conception.

Mise à niveau et informations sur le prix du Blueprint

À partir de la version 7.0, les profils de prix de vRealize Automation ne sont plus pris en charge et ne sont pas migrés vers le déploiement cible lors de la mise à niveau. Toutefois, vous pouvez exploiter l'intégration améliorée avec vRealize Business for Cloud pour gérer vos dépenses en ressources vRealize Automation.

vRealize Business for Cloud est désormais étroitement intégré à vRealize Automation et prend en charge les fonctionnalités de prix améliorées suivantes.

- Emplacement unifié dans vRealize Business for Cloud pour définir des stratégies de tarification flexibles pour :
 - Blueprints de ressource d'infrastructure, de machine et d'application.
 - Machines virtuelles provisionnées dans vRealize Automation pour des points de terminaison pris en charge, tels que vCenter Server, vCloud Director, Amazon Web Services, Azure et OpenStack.
 - Tout prix de fonctionnement, prix unique ou prix sur les propriétés personnalisées des machines virtuelles provisionnées.
 - Déploiements, y compris le prix des machines virtuelles dans les déploiements.
- Rapports d'analyse rétrospective basés sur les rôles dans vRealize Business for Cloud.
- Exploitation complète des nouvelles fonctionnalités de vRealize Business for Cloud.

Avant de procéder à la mise à niveau, vous pouvez exporter vos rapports de dépenses existants depuis votre instance vRealize Automation source pour référence. Une fois la mise à niveau terminée, vous pouvez installer et configurer vRealize Business for Cloud pour gérer les prix.

Note vRealize Automation est uniquement compatible avec la même version de vRealize Business for Cloud.

Mise à niveau et éléments de catalogue

Après la mise à niveau de vRealize Automation 6.2.x vers la version la plus récente, certains éléments du catalogue figurent dans le catalogue de services, mais ne sont pas disponibles pour les demandes.

Après la migration vers la dernière version de vRealize Automation, les éléments de catalogue qui utilisent ces définitions de propriété figurent dans le catalogue de services mais ne sont pas disponibles pour les demandes.

- Types de contrôle : case à cocher ou lien.
- Attributs : relation, expressions régulières ou dispositions de propriétés.

Dans vRealize Automation 7.x, les définitions de propriété n'utilisent plus ces éléments. Vous devez créer à nouveau la définition de propriété ou la configurer de sorte à utiliser une action de script vRealize Orchestrator au lieu des types de contrôle ou d'attributs intégrés. Pour plus d'informations, reportez-vous à [Des éléments de catalogue s'affichent dans le catalogue de services après la mise à niveau mais ne sont pas disponibles pour les demandes](#).

Liste de contrôle pour la mise à niveau de vRealize Automation

Lorsque vous effectuez une mise à niveau à partir de vRealize Automation 6.2.5, vous mettez à jour tous les composants vRealize Automation dans un ordre spécifique.

Utilisez les listes de contrôle pour faire le suivi de votre travail pendant la mise à niveau. Effectuez les tâches dans l'ordre dans lequel elles sont fournies.

Note Vous devez mettre à niveau tous les composants dans l'ordre indiqué. L'utilisation d'un ordre différent peut entraîner un comportement imprévu après la mise à niveau ou l'échec de la mise à niveau. Pour plus d'informations sur la documentation de mise à niveau de versions précédentes, consultez la [documentation du produit vRealize Automation](#).

L'ordre de mise à niveau varie selon que vous effectuez la mise à niveau d'un environnement minimal ou d'un environnement distribué comprenant plusieurs dispositifs vRealize Automation.

Tableau 1-61. Liste de contrôle de mise à niveau d'un environnement vRealize Automation minimal

Tâche	Instructions
<input type="checkbox"/> Sauvegardez votre installation actuelle. Cette sauvegarde constitue une tâche critique.	<p>Pour plus d'informations sur la sauvegarde et la restauration de votre système, reportez-vous à Sauvegarder votre environnement vRealize Automation 6.2.5 existant.</p> <p>Pour obtenir des informations générales, reportez-vous au document <i>Configuring Backup and Restore by Using Symantec NetBackup</i> (Configuration de la sauvegarde et la restauration à l'aide de Symantec NetBackup) à l'adresse http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf</p>
<input type="checkbox"/> Préparez les machines virtuelles vRealize Automation 6.2.x pour la mise à niveau.	Vous devez consulter l'article 51531 de la base de connaissances et effectuer tous les correctifs appropriés à vos environnements avant de procéder à la mise à niveau.
<input type="checkbox"/> Arrêtez les services Windows vRealize Automationsur votre serveur IaaS.	Reportez-vous à Arrêter les services vRealize Automation sur le serveur Windows IaaS .

Tableau 1-61. Liste de contrôle de mise à niveau d'un environnement vRealize Automation minimal (suite)

Tâche	Instructions
<input type="checkbox"/> Si le catalogue des composants communs est installé, vous devez le désinstaller avant de réaliser la mise à niveau.	<p>Pour en savoir plus sur la procédure de désinstallation des composants du catalogue de composants communs, reportez-vous au <i>Guide d'installation du catalogue de composants communs</i>.</p> <p>Si ce guide n'est pas disponible, procédez comme suit sur chaque nœud IaaS.</p> <ol style="list-style-type: none"> 1 Connectez-vous au nœud IaaS. 2 Cliquez sur Démarrer. 3 Entrez services dans la zone de texte Rechercher les programmes et fichiers. 4 Cliquez sur Services. 5 Dans le volet droit de la fenêtre Services, cliquez avec le bouton droit sur chaque service IaaS et sélectionnez Arrêter pour arrêter chaque service. 6 Cliquez sur Démarrer > Panneau de configuration > Programmes et fonctionnalités. 7 Cliquez avec le bouton droit sur chaque composant installé du Catalogue de composants communs, puis sélectionnez Désinstaller. 8 Cliquez sur Démarrer > Inviter de commandes. 9 À l'invite de commandes, exécutez iisreset.
<input type="checkbox"/> Consultez les considérations à prendre en compte concernant la mise à niveau vers cette version de vRealize Automation pour savoir ce qui peut être mis à niveau, ce qui ne peut pas être mis à niveau et comment les éléments mis à niveau peuvent se comporter différemment. Certains éléments, notamment les Blueprints, les réservations et les points de terminaison ne peuvent pas être mis à niveau. La présence de configurations non prises en charge bloque la mise à niveau.	<p>Reportez-vous à Remarques relatives à la mise à niveau vers cette version de vRealize Automation.</p>
<input type="checkbox"/> Configurez vos ressources matérielles.	<p>Reportez-vous à Augmenter les ressources matérielles de vCenter Server pour vRealize Automation 6.2.5.</p>
<input type="checkbox"/> Téléchargez les mises à jour sur le dispositif vRealize Automation.	<p>Reportez-vous à Téléchargement des mises à jour du dispositif vRealize Automation.</p>
<input type="checkbox"/> Installez la mise à jour sur le dispositif vRealize Automation.	<p>Reportez-vous à Installer la mise à jour sur dispositif vRealize Automation.</p>
<input type="checkbox"/> Mettez à jour l'utilitaire Single-Sign On vers l'utilitaire VMware Identity Manager.	<p>Reportez-vous à Mettre à jour votre mot de passe Single Sign-On pour VMware Identity Manager.</p>
<input type="checkbox"/> Mettez à jour la clé de licence.	<p>Reportez-vous à Mettre à jour la clé de licence.</p>
<input type="checkbox"/> Migrez le magasin d'identités vers l'instance de VMware Identity Manager.	<p>Reportez-vous à la section Migrer des magasins d'identités vers VMware Identity Manager.</p>

Tableau 1-61. Liste de contrôle de mise à niveau d'un environnement vRealize Automation minimal (suite)

Tâche	Instructions
<input type="checkbox"/> Mettez à niveau les composants IaaS.	Reportez-vous à Mise à niveau des composants du serveur IaaS après la mise à niveau de vRealize Automation .
<input type="checkbox"/> Migrez le vRealize Orchestrator externe.	Reportez-vous à Migration d'un vRealize Orchestrator 7.5 externe à externe dans le <i>Guide de migration de vRealize Orchestrator</i> .
<input type="checkbox"/> Ajoutez des utilisateurs ou des groupes à une connexion Active Directory.	Reportez-vous à Ajouter des utilisateurs ou des groupes à une connexion Active Directory .

Tableau 1-62. Liste de contrôle de mise à niveau d'un environnement vRealize Automation distribué

Tâche	Instructions
<input type="checkbox"/> Sauvegardez votre installation actuelle. Cette sauvegarde constitue une tâche critique.	<p>Pour plus d'informations sur la sauvegarde et la restauration de votre système, reportez-vous à Sauvegarder votre environnement vRealize Automation 6.2.5 existant.</p> <p>Pour obtenir des informations détaillées, reportez-vous au document <i>Configuring Backup and Restore by Using Symantec NetBackup</i> (Configuration de la sauvegarde et la restauration à l'aide de Symantec NetBackup) à l'adresse http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf</p>
<input type="checkbox"/> Préparez les machines virtuelles vRealize Automation 6.2.x pour la mise à niveau.	Vous devez vérifier l'article 51531 de la base de connaissances et effectuer tous les correctifs appropriés à vos environnements avant la mise à niveau.
<input type="checkbox"/> Arrêtez les services vRealize Automation sur vos serveurs IaaS Windows.	Reportez-vous à Arrêter les services vRealize Automation sur le serveur Windows IaaS .

Tableau 1-62. Liste de contrôle de mise à niveau d'un environnement vRealize Automation distribué (suite)

Tâche	Instructions
<input type="checkbox"/> Si le catalogue des composants communs est installé, vous devez le désinstaller avant de réaliser la mise à niveau.	<p>Pour en savoir plus sur la procédure de désinstallation des composants du catalogue de composants communs, reportez-vous au <i>Guide d'installation du catalogue de composants communs</i>.</p> <p>Si ce guide n'est pas disponible, procédez comme suit sur chaque nœud IaaS.</p> <ol style="list-style-type: none"> 1 Connectez-vous au nœud IaaS. 2 Cliquez sur Démarrer. 3 Entrez services dans la zone de texte Rechercher les programmes et fichiers. 4 Cliquez sur Services. 5 Dans le volet droit de la fenêtre Services, cliquez avec le bouton droit sur chaque service IaaS et sélectionnez Arrêter pour arrêter chaque service. 6 Cliquez sur Démarrer > Panneau de configuration > Programmes et fonctionnalités. 7 Cliquez avec le bouton droit sur chaque composant installé du Catalogue de composants communs, puis sélectionnez Désinstaller. 8 Cliquez sur Démarrer > Invite de commandes. 9 À l'invite de commandes, exécutez iisreset.
<input type="checkbox"/> Configurez vos ressources matérielles pour la mise à niveau.	<p>Reportez-vous à Augmenter les ressources matérielles de vCenter Server pour vRealize Automation 6.2.5.</p>
<input type="checkbox"/> Désactivez vos équilibres de charge.	<p>Désactivez chaque nœud secondaire et supprimez les moniteurs de santé de vRealize Automation pour les éléments suivants.</p> <ul style="list-style-type: none"> ■ Dispositif vRealize Automation ■ Site Web IaaS ■ IaaS Manager Service <p>Pour une mise à niveau réussie, vérifiez ce qui suit :</p> <ul style="list-style-type: none"> ■ Le trafic d'équilibrage de charge est uniquement dirigé vers le nœud principal. ■ Les moniteurs de santé vRealize Automation sont supprimés pour le dispositif, le site Web et Manager Service.
<input type="checkbox"/> Téléchargez les mises à jour sur le dispositif vRealize Automation.	<p>Reportez-vous à Téléchargement des mises à jour du dispositif vRealize Automation.</p>
<input type="checkbox"/> Installez la mise à jour sur le premier dispositif vRealize Automation de votre installation. Si un dispositif est désigné comme maître, mettez celui-ci à niveau en premier.	<p>Reportez-vous à Installer la mise à jour sur dispositif vRealize Automation.</p>
<input type="checkbox"/> Mettez à jour l'utilitaire Single-Sign On vers l'utilitaire VMware Identity Manager.	<p>Reportez-vous à Mettre à jour votre mot de passe Single Sign-On pour VMware Identity Manager.</p>

Tableau 1-62. Liste de contrôle de mise à niveau d'un environnement vRealize Automation distribué (suite)

Tâche	Instructions
<input type="checkbox"/> Mettez à jour la clé de licence.	Reportez-vous à Mettre à jour la clé de licence .
<input type="checkbox"/> Migrez le magasin d'identités vers l'utilitaire VMware Identity Manager.	Reportez-vous à la section Migrer des magasins d'identités vers VMware Identity Manager .
<input type="checkbox"/> Installez la mise à jour sur le reste de vos dispositifs vRealize Automation.	Reportez-vous à la section Installer la mise à jour sur des dispositifs vRealize Automation supplémentaires .
<input type="checkbox"/> Mettez à niveau les composants IaaS.	Reportez-vous à Mise à niveau des composants du serveur IaaS après la mise à niveau de vRealize Automation .
<input type="checkbox"/> Migrez le vRealize Orchestrator externe.	Reportez-vous à Migration d'un vRealize Orchestrator 7.5 externe à externe dans le <i>Guide de migration de vRealize Orchestrator</i> .
<input type="checkbox"/> Activez vos équilibres de charge.	Reportez-vous à la section Activer vos équilibres de charge .

Interfaces utilisateur de l'environnement vRealize Automation

Utilisez et gérez votre environnement vRealize Automation avec plusieurs interfaces.

interfaces utilisateur

Ces tableaux décrivent les interfaces qui permettent de gérer votre environnement vRealize Automation.

Tableau 1-63. Console d'administration vRealize Automation

Objectif	Accès	Informations d'identification requises
Utilisez la console vRealize Automation pour ces tâches de l'administrateur système.	1 Démarrez un navigateur et ouvrez la page de démarrage du dispositif vRealize Automation en utilisant le nom de domaine complet du dispositif virtuel :	Vous devez être un utilisateur disposant du rôle administrateur système.
■ Ajouter des locataires.		
■ Personnaliser l'interface utilisateur vRealize Automation.	https://vrealize-automation-appliance-FQDN .	
■ Configurer les serveurs de messagerie.	2 Cliquez sur vRealize Automation Console .	Vous pouvez également utiliser cette URL pour ouvrir la console vRealize Automation :
■ Afficher les journaux des événements.		
■ Configurez vRealize Orchestrator.	https://vrealize-automation-appliance-FQDN/vcac	
	3 Connectez-vous.	

Tableau 1-64. Console de locataire vRealize Automation. Cette interface est l'interface utilisateur principale que vous utilisez pour créer et gérer vos services et ressources.

Objectif	Accès	Informations d'identification requises
<p>Utilisez vRealize Automation pour ces tâches.</p> <ul style="list-style-type: none"> ■ Demander de nouveaux Blueprints de service informatique. ■ Créer et gérer des ressources cloud et informatiques. ■ Créer et gérer des groupes personnalisés. ■ Créer et gérer des groupes d'activité. ■ Attribuer des rôles aux utilisateurs 	<p>1 Démarrez un navigateur et entrez l'URL de votre locataire en utilisant le nom de domaine complet du dispositif virtuel et le nom de l'URL du locataire :</p> <p><code>https://vrealize-automation-appliance-FQDN/vcac/org/tenant_URL_name</code> .</p> <p>2 Connectez-vous.</p>	<p>Vous devez être un utilisateur disposant d'un ou de plusieurs de ces rôles :</p> <ul style="list-style-type: none"> ■ Architecte d'application ■ Administrateur d'approbations ■ Administrateur du catalogue ■ Administrateur de conteneur ■ Architecte de conteneur ■ Consommateur de santé ■ Architecte d'infrastructure ■ Consommateur d'exportation sécurisée ■ Architecte de logiciel ■ Administrateur de locataire ■ Architecte XaaS

Tableau 1-65. Interface de gestion du dispositif vRealize Automation.

Objectif	Accès	Informations d'identification requises
<p>Utilisez la gestion des dispositifs vRealize Automation pour ces tâches.</p> <ul style="list-style-type: none"> ■ Afficher l'état des services enregistrés. ■ Afficher les informations système et redémarrer ou arrêter le dispositif. ■ Gérer la participation au Programme d'amélioration du produit. ■ Afficher l'état du réseau. ■ Afficher l'état de mise à jour et installer les mises à jour. ■ Gérer les paramètres d'administration. ■ Gérer les paramètres de l'hôte vRealize Automation. ■ Gérer les paramètres SSO. ■ Gérer les licences des produits. ■ Configurer la base de données Postgres vRealize Automation. ■ Configurer la messagerie vRealize Automation. ■ Configurer la journalisation vRealize Automation. ■ Installer les composants IaaS. ■ Migrer à partir d'une installation vRealize Automation existante ■ Gérer les certificats des composants IaaS ■ Configurer le service Xenon. 	<ol style="list-style-type: none"> 1 Démarrez un navigateur et ouvrez la page de démarrage du dispositif vRealize Automation en utilisant le nom de domaine complet du dispositif virtuel : https://vrealize-automation-appliance-FQDN 2 Cliquez sur Gestion de dispositifs vRealize Automation. Vous pouvez également utiliser cette URL pour ouvrir l'interface de gestion du dispositif vRealize Automation : https://vrealize-automation-appliance-FQDN:5480 3 Connectez-vous. 	<ul style="list-style-type: none"> ■ Nom d'utilisateur : root ■ Mot de passe : mot de passe que vous avez entré lorsque vous avez déployé le dispositif vRealize Automation.

Tableau 1-66. Client vRealize Orchestrator

Objectif	Accès	Informations d'identification requises
<p>Utilisez le client vRealize Orchestrator pour effectuer ces tâches.</p> <ul style="list-style-type: none"> ■ Développer des actions. ■ Développer des workflows. ■ Gérer des stratégies. ■ Installer des modules. ■ Gérer les autorisations d'utilisateur et de groupe d'utilisateurs. ■ Attacher des balises à des objets URI. ■ Afficher l'inventaire. 	<ol style="list-style-type: none"> 1 Démarrez un navigateur et ouvrez la page de démarrage vRealize Automation en utilisant le nom de domaine complet du dispositif virtuel : https://vrealize-automation-appliance-FQDN 2 Pour télécharger le fichier client.jnlp sur votre ordinateur local, cliquez sur vRealize Orchestrator Client. 3 Cliquez avec le bouton droit de la souris sur le fichier client.jnlp et sélectionnez Lancer. 4 Dans la boîte de dialogue Voulez-vous continuer ?, cliquez sur Continuer. 5 Connectez-vous. 	<p>Vous devez être un utilisateur disposant du rôle d'administrateur système ou appartenir au groupe vcoadmins configuré dans les paramètres de fournisseur d'authentification du centre de contrôle vRealize Orchestrator.</p>

Tableau 1-67. Centre de contrôle vRealize Orchestrator

Objectif	Accès	Informations d'identification requises
<p>Utilisez le centre de contrôle vRealize Orchestrator pour modifier la configuration de l'instance par défaut de vRealize Orchestrator qui est intégrée dans vRealize Automation.</p>	<ol style="list-style-type: none"> 1 Démarrez un navigateur et ouvrez la page de démarrage du dispositif vRealize Automation en utilisant le nom de domaine complet du dispositif virtuel : https://vrealize-automation-appliance-FQDN 2 Cliquez sur Gestion de dispositifs vRealize Automation. Vous pouvez également utiliser cette URL pour ouvrir l'interface de gestion du dispositif vRealize Automation : https://vrealize-automation-appliance-FQDN:5480 3 Connectez-vous. 4 Cliquez sur vRA > Orchestrator. 5 Sélectionnez l'interface utilisateur d'Orchestrator. 6 Cliquez sur Démarrer. 7 Cliquez sur l'URL de l'interface utilisateur d'Orchestrator. 8 Connectez-vous. 	<p>Nom d'utilisateur</p> <ul style="list-style-type: none"> ■ Entrez root si l'authentification basée sur les rôles n'est pas configurée. ■ Entrez votre nom d'utilisateur vRealize Automation s'il est configuré pour l'authentification basée sur les rôles. <p>Mot de passe</p> <ul style="list-style-type: none"> ■ Entrez le mot de passe que vous avez entré lorsque vous avez déployé le dispositif vRealize Automation si l'authentification basée sur les rôles n'est pas configurée. ■ Entrez le mot de passe de votre nom d'utilisateur si ce dernier est configuré pour l'authentification basée sur les rôles.

Tableau 1-68. Invite de commande Linux

Objectif	Accès	Informations d'identification requises
<p>Utilisez l'invite de commande Linux sur un hôte, tels que l'hôte du dispositif vRealize Automation, pour ces tâches.</p> <ul style="list-style-type: none"> ■ Arrêter ou démarrer les services ■ Modifier les fichiers de configuration ■ Exécuter des commandes ■ Récupérer des données 	<ol style="list-style-type: none"> 1 Sur l'hôte du dispositif vRealize Automation, ouvrez une nouvelle invite de commande. Pour ouvrir l'invite de commande sur votre ordinateur local, vous pouvez démarrer une session sur l'hôte à l'aide d'une application telle que PuTTY. 2 Connectez-vous. 	<ul style="list-style-type: none"> ■ Nom d'utilisateur : root ■ Mot de passe : mot de passe que vous avez créé lorsque vous avez déployé le dispositif vRealize Automation.

Tableau 1-69. Invite de commande Windows

Objectif	Accès	Informations d'identification requises
<p>Vous pouvez utiliser une invite de commande Windows sur un hôte, tel que l'hôte IaaS, pour exécuter des scripts.</p>	<ol style="list-style-type: none"> 1 Sur l'hôte IaaS, connectez-vous à Windows. Pour vous connecter à partir de votre ordinateur local, vous pouvez démarrer une session de poste de travail distante. 2 Ouvrez l'invite de commande Windows. Pour ouvrir l'invite de commande, cliquez avec le bouton droit sur l'icône Démarrer sur l'hôte et sélectionnez Invite de commande ou Invite de commande (admin). 	<ul style="list-style-type: none"> ■ Nom d'utilisateur : utilisateur disposant de privilèges administratifs. ■ Mot de passe : mot de passe de l'utilisateur.

Mise à niveau de produits VMware intégrés à vRealize Automation

Vous devez gérer tous les produits VMware intégrés à votre environnement vRealize Automation lorsque vous procédez à la mise à niveau de vRealize Automation.

Si votre environnement vRealize Automation est intégré à un ou plusieurs autres produits, vous devez mettre à niveau vRealize Automation avant de mettre à jour les autres produits. Si vRealize Business for Cloud est intégré à vRealize Automation, vous devez annuler l'enregistrement de vRealize Business for Cloud avant de mettre à niveau vRealize Automation.

Suivez le workflow suggéré pour gérer les produits intégrés lorsque vous procédez à la mise à niveau de vRealize Automation.

- 1 Mettez à niveau vRealize Automation.
- 2 Mettez à niveau VMwarevRealize Operations Manager.
- 3 Mettez à niveau VMwarevRealize Log Insight.
- 4 Mettez à niveau VMwarevRealize Business for Cloud.

Cette section fournit des conseils supplémentaires sur la gestion de vRealize Business for Cloud lorsqu'il est intégré à votre environnement vRealize Automation.

Mise à niveau de vRealize Operations Manager intégré à vRealize Automation

Procédez à la mise à niveau de vRealize Operations Manager après avoir mis à niveau vRealize Automation.

Procédure

- 1 Mettez à niveau vRealize Automation.
- 2 Mettez à niveau vRealize Operations Manager. Pour plus d'informations, reportez-vous à la section *Mise à niveau de votre logiciel* dans la documentation de [VMware vRealize Operations Manager](#).

Mise à niveau de vRealize Log Insight intégré à vRealize Automation

Procédez à la mise à niveau de vRealize Log Insight après avoir mis à niveau vRealize Automation.

Procédure

- 1 Mettez à niveau vRealize Automation.
- 2 Mettez à niveau vRealize Log Insight. Pour plus d'informations, reportez-vous à la section *Mise à niveau de vRealize Log Insight* dans la documentation de [VMware vRealize Log Insight](#).

Mise à niveau de vRealize Business for Cloud intégré à vRealize Automation

Lorsque vous mettez à niveau votre environnement vRealize Automation, vous devez annuler l'enregistrement de votre connexion à vRealize Business for Cloud, puis enregistrer à nouveau la connexion.

Effectuez cette procédure pour garantir la continuité du service avec vRealize Business for Cloud lorsque vous mettez à niveau votre environnement vRealize Automation.

Procédure

- 1 Annulez l'enregistrement de vRealize Business for Cloud depuis vRealize Automation. Reportez-vous à la section *Annuler l'enregistrement de vRealize Business for Cloud depuis vRealize Automation* dans la documentation de [VMware vRealize Business for Cloud](#).
- 2 Mettez à niveau vRealize Automation.
- 3 Si nécessaire, mettez à niveau vRealize Business for Cloud. Reportez-vous à la section *Mise à niveau de vRealize Business for Cloud* dans la documentation de [VMware vRealize Business for Cloud](#).
- 4 Enregistrez vRealize Business for Cloud dans vRealize Automation. Reportez-vous à la section *Enregistrer vRealize Business for Cloud avec vRealize Automation* dans la documentation de [VMware vRealize Business for Cloud](#).

Préparation de la mise à niveau de vRealize Automation

Vous devez effectuer diverses tâches et procédures avant de mettre à niveau vRealize Automation 6.2.5.

Effectuez les tâches dans l'ordre indiqué dans la liste de contrôle de mise à niveau. Reportez-vous à [Liste de contrôle pour la mise à niveau de vRealize Automation](#).

Conditions préalables de sauvegarde pour la mise à niveau de vRealize Automation

Remplissez les conditions préalables de sauvegarde avant de mettre à niveau vRealize Automation 6.2.5.

Conditions préalables

- Vérifiez que l'environnement source est entièrement installé et configuré.
- Pour chaque dispositif dans l'environnement source, sauvegardez tous les fichiers de configuration du dispositif vRealize Automation dans les répertoires suivants.
 - `/etc/vcac/`
 - `/etc/vco/`
 - `/etc/apache2/`
 - `/etc/rabbitmq/`
- Sauvegardez les fichiers de configuration du workflow externe (xmldb) de vRealize Automation sur votre système. Stockez les fichiers de sauvegarde dans un répertoire temporaire. Ces fichiers se trouvent ici : `\VMware\vCA\Server\ExternalWorkflows\xmldb\`. Vous restaurez les fichiers xmldb sur votre nouveau système après la migration. Reportez-vous à [Restaurer les fichiers de délai d'expiration du workflow externe](#).

 Pour un problème lié, reportez-vous à [Copies de sauvegarde de fichiers .xml entraînant l'expiration du délai du système](#).
- Sauvegardez la base de données PostgreSQL externe de vRealize Automation. Pour voir si votre base de données PostgreSQL est externe, exécutez la procédure suivante.
 - a Connectez-vous en tant qu'utilisateur racine à l'interface de gestion du dispositif vRealize Automation principal ou master.

`https://vrealize-automation-appliance-FQDN:5480`
 - b Sélectionnez **Cluster**.
 - c Si l'hôte du nœud de base de données PostgreSQL vRealize Automation est différent de l'hôte du dispositif vRealize Automation, sauvegardez la base de données. Si l'hôte du nœud de base de données est identique à l'hôte du dispositif, vous n'avez pas besoin de sauvegarder la base de données.

 Pour plus d'informations sur la sauvegarde de la base de données PostgreSQL, reportez-vous à <https://www.postgresql.org/>.
- Créez un snapshot de votre configuration des locataires et des utilisateurs attribués.
- Sauvegardez tous les fichiers que vous avez personnalisés, par exemple `DataCenterLocations.xml`.

- Créez un snapshot de chaque dispositif virtuel et de chaque serveur IaaS. Suivez les directives standard relatives à la sauvegarde de l'intégralité du système en cas d'échec de la mise à niveau de vRealize Automation. Reportez-vous à [Sauvegarde et récupération des installations de vRealize Automation](#).

Sauvegarder votre environnement vRealize Automation 6.2.5 existant

Avant de procéder à la mise à niveau, arrêtez la machine et prenez un snapshot des composants de votre environnement vRealize Automation 6.2.5.

Avant de procéder à la mise à niveau, prenez un snapshot de ces composants pendant la mise à l'arrêt du système.

- Serveurs vRealize Automation IaaS (nœuds Windows)
- Dispositifs vRealize Automation (nœuds Linux)
- Nœud d'identité vRealize Automation (SSO)

Si la mise à niveau échoue, utilisez le snapshot pour revenir à la dernière configuration correcte connue et tentez une nouvelle mise à niveau.

Conditions préalables

- Vérifiez que la base de données PostgreSQL intégrée est en mode haute disponibilité. Si c'est le cas, localisez le nœud master actuel. Consultez l'article de la base de connaissance <http://kb.vmware.com/kb/2105809>.
- Si votre environnement dispose d'une base de données PostgreSQL externe, créez un fichier de sauvegarde de base de données.
- Si la base de données Microsoft SQL de vRealize Automation n'est pas hébergée sur le serveur IaaS, créez un fichier de sauvegarde de base de données. Pour plus d'informations, recherchez l'article sur [Microsoft Developer Network](#) concernant la création d'une sauvegarde complète de la base de données SQL Server.
- Vérifiez que vous remplissez les conditions requises de sauvegarde pour la mise à niveau.
- Vérifiez que vous avez créé un snapshot de votre système pendant qu'il est à l'arrêt. C'est la méthode préférée de prise d'un snapshot. Pour plus d'informations sur la création et la gestion de snapshots, reportez-vous à la [documentation du produit vSphere](#).

Note Lorsque vous sauvegardez le dispositif vRealize Automation et les composants IaaS, désactivez les snapshots en mémoire et les snapshots mis au repos.

- Si vous avez modifié le fichier `app.config`, sauvegardez ce fichier. Reportez-vous à [Restaurer les modifications apportées à la connexion dans le fichier app.config](#).
- Sauvegardez les fichiers de configuration du workflow externe (xmldb). Reportez-vous à [Restaurer les fichiers de délai d'expiration du workflow externe](#).
- Vérifiez que vous disposez d'un emplacement à l'extérieur de votre dossier actuel dans lequel vous pouvez stocker votre fichier de sauvegarde. Reportez-vous à [Copies de sauvegarde de fichiers .xml entraînant l'expiration du délai du système](#).

Procédure

- 1 Connectez-vous à votre système vCenter Server.
- 2 Recherchez ces composants vRealize Automation 6.2.5.
 - Serveurs vRealize Automation IaaS (nœuds Windows)
 - Dispositifs vRealize Automation (nœuds Linux)
 - Nœud d'identité vRealize Automation (SSO)
- 3 Pour chacune des machines virtuelles suivantes, sélectionnez la machine virtuelle et cliquez sur **Arrêter invité**, puis attendez que la machine s'arrête. Arrêtez ces machines virtuelles dans l'ordre suivant.
 - a machines virtuelles de l'agent proxy IaaS
 - b machines virtuelles DEM Worker
 - c machine virtuelle DEM Orchestrator
 - d machine virtuelle Manager Service
 - e machines virtuelles Web Service
 - f Dispositifs virtuels vRealize Automation secondaires
 - g Dispositif virtuel vRealize Automation principal
 - h machines virtuelles Manager (le cas échéant)
 - i Identity Appliance
- 4 Prenez un snapshot de chaque machine virtuelle vRealize Automation 6.2.5.
- 5 Clonez chaque nœud de dispositif vRealize Automation.

Vous effectuez la mise à niveau sur les machines virtuelles clonées.
- 6 Mettez hors tension chaque machine virtuelle de dispositif vRealize Automation d'origine avant de mettre à niveau les machines virtuelles clonées.

Maintenez les machines virtuelles d'origine hors tension et utilisez-les uniquement si vous devez restaurer le système.

Étape suivante

[Augmenter les ressources matérielles de vCenter Server pour vRealize Automation 6.2.5.](#)

Augmenter les ressources matérielles de vCenter Server pour vRealize Automation 6.2.5

Avant de procéder à la mise à niveau de vRealize Automation 6.2.5, vous devez augmenter les ressources matérielles pour chaque dispositif vRealize Automation.

Cette procédure part du principe que vous utilisez le client Windows vCenter Server.

Conditions préalables

- Vérifiez que vous disposez d'un clone de chaque dispositif vRealize Automation.

- Vérifiez que vous disposez d'au moins 140 Go d'espace libre dans votre système vCenter Server pour chaque clone de dispositif.
- Vérifiez que les dispositifs d'origine sont mis hors tension.

Procédure

- 1 Connectez-vous à vCenter Server.
- 2 Cliquez avec le bouton droit sur une icône de dispositif vRealize Automation cloné et sélectionnez **Modifier les paramètres**.
- 3 Sélectionnez **Mémoire** et réglez la valeur sur 18 Go.
- 4 Sélectionnez **CPU** et réglez la valeur **Nombre de sockets virtuels** sur 4.
- 5 Portez la taille du disque virtuel 1 à 50 Go.
 - a Sélectionnez le Disque 1.
 - b Modifiez la taille et choisissez 50 Go.
 - c Cliquez sur **OK**.
- 6 Si vous n'avez pas de Disque 3, procédez comme suit pour ajouter un Disque 3 d'une taille de 25 Go.
 - a Cliquez sur **Ajouter** au-dessus du tableau Ressources pour ajouter un disque virtuel.
 - b Sélectionnez **Disque dur** pour **Type de périphérique**, puis cliquez sur **Suivant**.
 - c Sélectionnez **Créer un disque virtuel**, puis cliquez sur **Suivant**.
 - d Réglez la valeur **Taille de disque** sur 25 Go.
 - e Sélectionnez **Stocker avec la machine virtuelle**, puis cliquez sur **Suivant**.
 - f Vérifiez que l'option **Indépendant** n'est pas sélectionnée pour **Mode** et que **SCSI (0:2)** est sélectionnée pour **Mode de dispositif virtuel**, puis cliquez sur **Suivant**.
Si vous êtes invité à accepter les paramètres recommandés, acceptez-les.
 - g Cliquez sur **Terminer**.
 - h Cliquez sur **OK**.
- 7 En présence d'un disque virtuel 4 d'une version précédente de vRealize Automation, procédez comme suit.
 - a Mettez sous tension le clone du dispositif virtuel principal et attendez une minute.
 - b Mettez sous tension le clone du dispositif virtuel secondaire.
 - c Sur le clone du dispositif virtuel principal, ouvrez une nouvelle invite de commandes et accédez à `/etc/fstab`.
 - d Sur le clone du dispositif virtuel principal, ouvrez le fichier `fstab` et supprimez les lignes commençant par `/dev/sdd` qui contiennent les journaux WAL (Write Ahead Logs) `Wal_Archive`.

- e Sur le clone du dispositif virtuel principal, enregistrez le fichier.
 - f Sur le clone du dispositif virtuel secondaire, ouvrez une nouvelle invite de commandes et accédez à `/etc/fstab`.
 - g Sur le clone du dispositif virtuel secondaire, ouvrez le fichier `fstab` et supprimez les lignes commençant par `/dev/sdd` qui contiennent les journaux WAL (Write Ahead Logs) `Wal_Archive`.
 - h Sur le clone du dispositif virtuel secondaire, enregistrez le fichier.
 - i Mettez hors tension le clone du dispositif virtuel secondaire et attendez une minute.
 - j Mettez hors tension le clone du dispositif virtuel principal.
 - k Cliquez avec le bouton droit sur l'icône du dispositif vRealize Automation principal cloné et sélectionnez **Modifier les paramètres**.
 - l Supprimez le Disque 4 sur la machine du dispositif virtuel principal cloné.
 - m Cliquez avec le bouton droit sur l'icône du dispositif vRealize Automation secondaire cloné et sélectionnez **Modifier les paramètres**.
 - n Supprimez le Disque 4 sur la machine du dispositif virtuel secondaire cloné.
- 8** Répétez ces étapes pour ajouter un Disque 4 avec une taille de disque de 50 Go aux machines de dispositifs virtuels principal et secondaire clonés.
- a Cliquez sur **Ajouter** au-dessus du tableau Ressources pour ajouter un disque virtuel.
 - b Sélectionnez **Disque dur** pour **Type de périphérique**, puis cliquez sur **Suivant**.
 - c Sélectionnez **Créer un disque virtuel**, puis cliquez sur **Suivant**.
 - d Réglez la valeur **taille de disque** sur 50 Go.
 - e Sélectionnez **Stocker avec la machine virtuelle**, puis cliquez sur **Suivant**.
 - f Vérifiez que l'option **Indépendant** n'est pas sélectionnée pour **Mode** et que **SCSI (0:3)** est sélectionnée pour **Mode de dispositif virtuel**, puis cliquez sur **Suivant**.
- Si vous êtes invité à accepter les paramètres recommandés, acceptez-les.
- g Cliquez sur **Terminer**.
 - h Cliquez sur **OK**.
- 9** Créez un snapshot de la machine du dispositif virtuel principal cloné et de la machine du dispositif virtuel secondaire cloné.

Étape suivante

[Mettre l'ensemble du système sous tension.](#)

Mettre l'ensemble du système sous tension

Après avoir augmenté les ressources matérielles vCenter en vue d'une mise à niveau, vous devez mettre le système sous tension avant de procéder à la mise à niveau.

Conditions préalables

- [Sauvegarder votre environnement vRealize Automation 6.2.5 existant.](#)
- [Augmenter les ressources matérielles de vCenter Server pour vRealize Automation 6.2.5.](#)

Procédure

- 1 Mettez l'ensemble du système sous tension.

Pour obtenir des instructions, reportez-vous à la version 6.2 de vRealize Automation de la rubrique *Démarrer vRealize Automation*

Note Si vous disposez d'un environnement à haute disponibilité, utilisez cette procédure pour mettre sous tension vos dispositifs virtuels.

- a Mettez sous tension le dispositif virtuel que vous avez mis hors tension en dernier.
 - b Attendez une minute.
 - c Mettez sous tension les autres dispositifs virtuels.
-

- 2 Vérifiez que le système est entièrement fonctionnel.

Étape suivante

[Arrêter les services vRealize Automation sur le serveur Windows IaaS.](#)

Arrêter les services vRealize Automation sur le serveur Windows IaaS

Lorsque cela est nécessaire, vous pouvez utiliser la procédure suivante pour arrêter les services vRealize Automation sur chaque serveur qui exécute les services IaaS.

Avant de commencer la mise à niveau, arrêtez les services vRealize Automation sur chaque serveur Windows IaaS.

Note À l'exception d'une instance de sauvegarde passive du service du gestionnaire, le type de démarrage de tous les services doit être défini sur Automatique pendant le processus de mise à niveau. Si vous définissez des services sur Manuel, le processus de mise à niveau échoue.

Procédure

- 1 Connectez-vous à votre serveur Windows IaaS.
- 2 Sélectionnez **Démarrer > Outils d'administration > Services**.
- 3 Arrêtez les services dans l'ordre suivant. Veillez à ne pas arrêter la machine virtuelle.

Chaque machine virtuelle dispose d'un agent de gestion qui doit être arrêté avec chaque ensemble de services.

- a Chaque agent VMware vCloud Automation Center
- b Chaque VMware DEM-Worker
- c VMware DEM-Orchestrator

d Le service VMware vCloud Automation Center

- 4 Pour les déploiements distribués avec équilibrages de charge, désactivez tous les nœuds secondaires et supprimez les moniteurs de santé de vRealize Automation pour les éléments suivants.

a Dispositif vRealize Automation

b Site Web IaaS

c IaaS Manager Service

Assurez-vous que le trafic d'équilibrage de charge est dirigé uniquement vers les nœuds principaux et que les moniteurs de santé de vRealize Automation sont supprimés du dispositif, du site Web et de Manager Service, sinon la mise à niveau échoue.

- 5 Pour vérifier que le service IaaS hébergé dans Microsoft Internet Information Services (IIS) s'exécute, procédez comme suit :

a Dans votre navigateur, accédez à l'URL

<https://webhostname/Repository/Data/MetaModel.svc> pour vérifier que le référentiel Web s'exécute. S'il fonctionne correctement, aucune erreur n'est retournée et une liste des modèles au format XML s'affiche.

b Vérifiez que l'état enregistré dans le fichier `Repository.log` sur le nœud Web de la machine virtuelle IaaS indique OK. Le fichier se trouve dans le dossier de base VCAC dans `/Server/Model Manager Web/Logs/Repository.log`.

Pour un site Web IaaS distribué, connectez-vous au site Web secondaire, sans MMD, puis arrêtez temporairement le serveur Microsoft IIS. Vérifiez la connectivité de `MetaModel.svc`. Pour vérifier que le trafic d'équilibrage de charge passe uniquement par le nœud Web principal, démarrez le serveur Microsoft IIS.

Étape suivante

[Téléchargement des mises à jour du dispositif vRealize Automation.](#)

Téléchargement des mises à jour du dispositif vRealize Automation

Recherchez les mises à jour dans l'interface de gestion du dispositif vRealize Automation et téléchargez-les en utilisant l'une des méthodes suivantes.

Pour garantir les meilleures performances de mise à niveau, utilisez la méthode du fichier ISO.

Pour éviter les problèmes potentiels lors de la mise à niveau de votre dispositif, ou si des problèmes surgissent pendant la mise à niveau du dispositif, reportez-vous à [l'article de la base de connaissances VMware](#) *La mise à niveau de vRealize Automation échoue en raison des doublons dans la base de données de vRealize Orchestrator (54987)*.

- [Télécharger les mises à jour du dispositif vRealize Automation dans un référentiel VMware](#)

Vous pouvez télécharger la mise à jour de votre dispositif vRealize Automation à partir d'un référentiel public sur le site Web [vmware.com](https://www.vmware.com).

- **Télécharger les mises à jour de dispositif virtuel pour une utilisation avec un lecteur de CD-ROM**

Vous pouvez mettre à jour votre dispositif virtuel à partir d'un fichier ISO que le dispositif lit à partir du lecteur de CD-ROM virtuel. C'est la méthode préférée.

Télécharger les mises à jour du dispositif vRealize Automation dans un référentiel VMware

Vous pouvez télécharger la mise à jour de votre dispositif vRealize Automation à partir d'un référentiel public sur le site Web vmware.com.

Conditions préalables

- Sauvegardez votre environnement vRealize Automation existant.
- Vérifiez que votre dispositif vRealize Automation est sous tension.

Procédure

- 1 Sur votre dispositif vRealize Automation principal, connectez-vous à la gestion des dispositifs vRealize Automation en tant qu'utilisateur **racine** à l'aide du mot de passe que vous avez entré lorsque vous avez déployé le dispositif vRealize Automation.
- 2 Cliquez sur l'onglet **Mettre à jour**.
- 3 Cliquez sur **Paramètres**.
- 4 (Facultatif) Définissez la fréquence de vérification des mises à jour dans le volet Mises à jour automatiques.
- 5 Dans le volet Référentiel de mises à jour, sélectionnez **Utiliser le référentiel par défaut**.
Le référentiel par défaut est défini sur l'URL correcte VMware.com.
- 6 Cliquez sur **Enregistrer les paramètres**.

Télécharger les mises à jour de dispositif virtuel pour une utilisation avec un lecteur de CD-ROM

Vous pouvez mettre à jour votre dispositif virtuel à partir d'un fichier ISO que le dispositif lit à partir du lecteur de CD-ROM virtuel. C'est la méthode préférée.

Vous téléchargez le fichier ISO et configurez le dispositif principal afin d'utiliser ce fichier pour mettre à niveau votre dispositif.

Conditions préalables

- Sauvegardez votre environnement vRealize Automation existant.
- Vérifiez que tous les lecteurs de CD-ROM utilisés dans votre mise à niveau sont activés avant de procéder à la mise à jour d'un dispositif vRealize Automation. Reportez-vous à la documentation de vSphere pour obtenir des informations sur l'ajout d'un lecteur de CD-ROM à une machine virtuelle dans le client vSphere.

Procédure

- 1 Téléchargez le fichier ISO du référentiel de mise à jour.
 - a Démarrez un navigateur et accédez à la [page du produit vRealize Automation](#) à l'adresse www.vmware.com.
 - b Cliquez sur **Ressources de téléchargement de vRealize Automation** pour accéder à la page de téléchargement de VMware.
 - c Téléchargez le fichier approprié.
- 2 Localisez le fichier téléchargé sur votre système pour vérifier que la taille du fichier est la même que celle du fichier de la page de téléchargement VMware. Utilisez les totaux de contrôle fournis sur la page de téléchargement pour valider l'intégrité du fichier téléchargé. Pour plus d'informations, reportez-vous aux liens figurant en bas de la page de téléchargement VMware.
- 3 Vérifiez que votre dispositif virtuel principal est sous tension.
- 4 Connectez le lecteur de CD-ROM du dispositif virtuel principal au fichier ISO que vous avez téléchargé.

Note Connectez-vous au dispositif et montez le CD-ROM dans Linux à l'aide de ce chemin de fichier `mount/dev/sr0/media/cdrom` si vous ne pouvez pas voir la mise à jour une fois que le fichier ISO est attaché à la machine virtuelle.

- 5 Sur votre dispositif vRealize Automation principal, connectez-vous à la gestion des dispositifs vRealize Automation en tant qu'utilisateur **racine** à l'aide du mot de passe que vous avez entré lorsque vous avez déployé le dispositif vRealize Automation.
- 6 Cliquez sur l'onglet **Mettre à jour**.
- 7 Cliquez sur **Paramètres**.
- 8 Sous Référentiel de mises à jour, sélectionnez **Utiliser les mises à jour de CD-ROM**.
- 9 Cliquez sur **Enregistrer les paramètres**.

Mise à jour du dispositif vRealize Automation

Après avoir réuni les conditions préalables de mise à niveau et téléchargé la mise à jour du dispositif virtuel, vous mettez à jour le dispositif vRealize Automation 6.2.5 vers la version actuelle.

Vous reconfigurez également certains paramètres pour le dispositif vRealize Automation principal.

Après la mise à niveau du dispositif vRealize Automation principal, vous mettez à niveau les autres nœuds de votre environnement dans l'ordre suivant :

- 1 Chaque dispositif vRealize Automation secondaire.
- 2 Site Web IaaS.

- 3 IaaS Manager Service.
- 4 DEM IaaS.
- 5 Agent IaaS.
- 6 Mettez à niveau ou migrez chaque instance externe de vRealize Orchestrator

Installer la mise à jour sur dispositif vRealize Automation

Vous installez la mise à jour de vRealize Automation sur le dispositif vRealize Automation 6.2.5 et configurez les paramètres du dispositif.

La prise en charge d'une base de données PostgreSQL externe est interrompue à partir de vRealize Automation 7.1. Le processus de mise à niveau fusionne les données d'une base de données PostgreSQL externe existante avec la base de données PostgreSQL interne faisant partie du dispositif vRealize Automation.

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>.

Ne fermez pas l'interface de gestion du dispositif vRealize Automation pendant que vous installez la mise à jour.

Si vous rencontrez des problèmes pendant le processus de mise à niveau, reportez-vous à [Résolution des problèmes de mise à niveau de vRealize Automation](#).

Conditions préalables

- Vérifiez que vous avez sélectionné une méthode de téléchargement et téléchargé la mise à jour. Reportez-vous à [Téléchargement des mises à jour du dispositif vRealize Automation](#).
- Pour les déploiements distribués à haute disponibilité, reportez-vous à [Sauvegarder votre environnement vRealize Automation 6.2.5 existant](#).
- Pour les déploiements incluant des équilibres de charge, vérifiez que le trafic est uniquement dirigé vers le nœud principal et que les moniteurs de santé sont désactivés.
- Si vous avez installé un composant du catalogue de composants communs dans votre environnement, désinstallez-le avant la mise à niveau. Pour plus d'informations, reportez-vous au *Guide d'installation du catalogue de composants communs*. Si ce guide n'est pas disponible, utilisez la procédure de remplacement dans [Liste de contrôle pour la mise à niveau de vRealize Automation](#).
- Vérifiez que la connexion de la base de données jdbc:postgresql pointe vers l'adresse IP externe du nœud master PostgreSQL.
 - a Sur chaque dispositif vRealize Automation, ouvrez une nouvelle invite de commandes.
 - b Accédez à `/etc/vcac/server.xml`, puis sauvegardez `server.xml`.
 - c Ouvrez `server.xml`.

- d Si nécessaire, modifiez l'entrée du fichier `server.xml` `jdbc:postgresql` qui pointe vers la base de données Postgres et pointez-la vers l'adresse IP externe du nœud master PostgreSQL pour la base de données PostgreSQL externe ou du dispositif virtuel principal pour la base de données PostgreSQL intégrée.

Par exemple, `jdbc:postgresql://198.15.100.60:5432/vcac`

- Vérifiez que toutes les demandes enregistrées et en cours sont terminées avec succès avant de procéder à la mise à niveau.

Procédure

- 1 Ouvrez l'interface de gestion du dispositif vRealize Automation.
 - a Sur votre dispositif vRealize Automation principal, connectez-vous à la gestion des dispositifs vRealize Automation en tant qu'utilisateur **racine** à l'aide du mot de passe que vous avez entré lorsque vous avez déployé le dispositif vRealize Automation.
 - b Connectez-vous avec le nom d'utilisateur **root** et le mot de passe que vous avez entrés lors du déploiement du dispositif.
- 2 Cliquez sur **Services** et vérifiez que tous les services, sauf `iaas-service`, sont répertoriés comme étant ENREGISTRÉS.
- 3 Sélectionnez **Mettre à jour > Paramètres**.
- 4 Sélectionnez l'une des options suivantes :
 - **Utilisez le référentiel par défaut.**
 - **Utiliser les mises à jour sur CDROM**
- 5 Cliquez sur **Enregistrer les paramètres**.
- 6 Sélectionnez **Statut**.
- 7 Cliquez sur **Vérifier les mises à jour** pour vérifier qu'une mise à jour est accessible.
- 8 (Facultatif) Pour des instances du dispositif vRealize Automation, cliquez sur **Détails** dans la zone Version du dispositif pour afficher les informations sur l'emplacement des notes de mise à jour.
- 9 Cliquez sur **Installer les mises à jour**.
- 10 Cliquez sur **OK**.

Un message indiquant que la mise à jour est en cours s'affiche.

- 11** (Facultatif) Si vous n'avez pas redimensionné Disque 1 à 50 Go manuellement, procédez comme suit.
- a Lorsque le système vous invite à redémarrer le dispositif virtuel, cliquez sur **Système**, puis sur **Redémarrer**.
Pendant le redémarrage, le système ajuste l'espace requis pour la mise à jour.
 - b Après le redémarrage du système, reconnectez-vous à l'interface de gestion du dispositif vRealize Automation, vérifiez que tous les services, sauf iaas-service, sont répertoriés comme étant ENREGISTRÉ, puis sélectionnez **Mettre à jour > État**.
 - c Cliquez sur **Vérifier les mises à jour** et **Installer les mises à jour**.

- 12** Pour afficher l'état de la mise à niveau, ouvrez les fichiers journaux suivants.

- /opt/vmware/var/log/vami/updatecli.log
- /opt/vmware/var/log/vami/vami.log
- /var/log/vmware/horizon/horizon.log
- /var/log/bootstrap/*.log

Pendant le processus de mise à niveau, si vous vous déconnectez et que vous vous reconnectez avant la fin de la mise à niveau, vous pouvez continuer de suivre la progression de la mise à jour dans le fichier journal. Le fichier updatecli.log peut afficher des informations sur la version de vRealize Automation à partir de laquelle vous effectuez la mise à niveau. Cette version affichée devient la version appropriée plus tard pendant le processus de mise à niveau.

Le temps requis pour terminer la mise à jour dépend de votre environnement.

- 13** Cliquez sur **Télémétrie** dans l'interface de gestion du dispositif vRealize Automation. Lisez la remarque relative à la participation au programme d'amélioration du produit et choisissez de rejoindre ou non le programme.

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>.

Pour plus d'informations sur le Programme d'amélioration du produit, reportez-vous à la section [Rejoindre ou quitter le Programme d'amélioration du produit pour vRealize Automation](#).

Étape suivante

[Mettre à jour votre mot de passe Single Sign-On pour VMware Identity Manager](#).

Mettre à jour votre mot de passe Single Sign-On pour VMware Identity Manager

Après avoir installé les mises à jour, vous devez mettre à jour le mot de passe Single Sign-On pour VMware Identity Manager.

VMware Identity Manager remplace les composants SSO Identity Appliance et vSphere.

Procédure

- 1 Déconnectez-vous de l'interface de gestion du dispositif vRealize Automation, fermez le navigateur, rouvrez-le et reconnectez-vous.
- 2 Sélectionnez **vRA > SSO**.
- 3 Entrez un nouveau mot de passe VMware Identity Manager et cliquez sur **Enregistrer les paramètres**.

N'utilisez pas de mots de passe simples. Vous pouvez ignorer en toute sécurité le message d'erreur Le serveur SSO n'est pas connecté. Plusieurs minutes peuvent être nécessaires pour redémarrer les services .

Le mot de passe est accepté.

Pour un déploiement à haute disponibilité, le mot de passe est appliqué au premier nœud du dispositif vRealize Automation et propagé à tous les nœuds secondaires du dispositif vRealize Automation.

- 4 Redémarrez le dispositif virtuel.
 - a Cliquez sur l'onglet **Système**.
 - b Cliquez sur **Redémarrer** et confirmez votre sélection.
- 5 Vérifiez que tous les services sont en cours d'exécution.
 - a Connectez-vous à l'interface de gestion du dispositif vRealize Automation.
 - b Cliquez sur l'onglet **Services** sur la console.
 - c Cliquez sur l'onglet **Actualiser** pour suivre la progression du démarrage des services.

Vous devez voir 35 services au minimum.

- 6 Assurez-vous que tous les services sont enregistrés, à l'exception d'iaas-service.

Le service release-management ne démarre pas sans une clé de licence vRealize Code Stream.

Étape suivante

[Mettre à jour la clé de licence.](#)

Mettre à jour la clé de licence

Vous devez mettre à niveau votre clé de licence pour utiliser la dernière version du dispositif vRealize Automation.

Procédure

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

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

2 Cliquez sur vRA > Attribution de licence.

Si l'onglet **Attribution de licence** n'est pas disponible, procédez comme suit et répétez la procédure.

- a Déconnectez-vous de l'interface de gestion.
- b Effacez le cache du navigateur.

3 Entrez votre nouvelle clé de licence dans la zone de texte Nouvelle clé de licence.

Les points de terminaison et les quotas sont indiqués conformément à votre contrat de licence d'utilisateur final (EULA).

4 Cliquez sur Envoyer la clé.**Étape suivante**

[Migrer des magasins d'identités vers VMware Identity Manager.](#)

Migrer des magasins d'identités vers VMware Identity Manager

Lorsque vous procédez à la mise à niveau de vRealize Automation 6.2.5 vers la version actuelle, vous devez migrer les magasins d'identités.

Si les procédures suivantes l'exigent, reportez-vous au snapshot des informations de votre configuration de locataire 6.2.5.

Note Après la migration des magasins d'identités, les utilisateurs de vRealize Code Stream doivent manuellement réattribuer des rôles vRealize Code Stream.

Procédure**1 [Créer un compte d'utilisateur local pour vos locataires](#)**

Vous devez configurer un locataire avec un compte d'utilisateur local et attribuer des privilèges d'administrateur de locataire au compte d'utilisateur local.

2 [Synchroniser les utilisateurs et les groupes pour un lien Active Directory](#)

Pour importer vos utilisateurs et vos groupes dans vRealize Automation en utilisant la fonctionnalité Gestion des annuaires, vous devez vous connecter à votre lien Active Directory.

3 [Migrer des groupes personnalisés vers l'instance cible de VMware Identity Manager](#)

Vous devez migrer tous les groupes personnalisés de l'environnement source vers VMware Identity Manager (vIDM) dans le déploiement cible.

4 [Migrer plusieurs locataires et administrateurs IaaS](#)

Pour chaque locataire vRealize Automation avec administrateurs de locataires ou administrateurs IaaS, vous devez supprimer et restaurer manuellement chaque administrateur.

Créer un compte d'utilisateur local pour vos locataires

Vous devez configurer un locataire avec un compte d'utilisateur local et attribuer des privilèges d'administrateur de locataire au compte d'utilisateur local.

Répétez cette procédure pour chacun de vos locataires.

Conditions préalables

Vérifiez que vous avez défini un nouveau mot de passe pour VMware Identity Manager.

Reportez-vous à [Mettre à jour votre mot de passe Single Sign-On pour VMware Identity Manager](#).

Procédure

- 1 Connectez-vous à la console vRealize Automation avec le nom d'utilisateur d'administrateur système **administrator** et le mot de passe par défaut.

L'emplacement de la console est `https://vra-appliance/vcac/`.

- 2 Cliquez sur votre locataire.

Par exemple, pour le locataire par défaut, cliquez sur **vsphere.local**

- 3 Sélectionnez l'onglet **Utilisateurs locaux**.

- 4 Cliquez sur **Nouveau**.

- 5 Créez un compte d'utilisateur local.

Vous attribuez le rôle d'administrateur de locataire à cet utilisateur. Vérifiez que le nom d'utilisateur local est propre à l'annuaire Active Directory vsphere.local.

- 6 Cliquez sur **OK**.

- 7 Cliquez sur **Administrateurs**.

- 8 Entrez le nom d'utilisateur local dans la zone de recherche **Administrateurs de locataire** et appuyez sur Entrée.

- 9 Cliquez sur **Terminer**.

- 10 Déconnectez-vous de la console.

Étape suivante

[Synchroniser les utilisateurs et les groupes pour un lien Active Directory](#).

Synchroniser les utilisateurs et les groupes pour un lien Active Directory

Pour importer vos utilisateurs et vos groupes dans vRealize Automation en utilisant la fonctionnalité Gestion des annuaires, vous devez vous connecter à votre lien Active Directory.

Exécutez cette procédure pour chacun de vos locataires.

Conditions préalables

Vérifiez que vous disposez de privilèges d'accès à l'annuaire Active Directory.

Procédure

- 1 Connectez-vous à la console vRealize Automation à l'adresse :
`https://vra-appliance/vcac/org/tenant_name`.
- 2 Sélectionnez **Administration > Gestion des annuaires > Annuaires**.
- 3 Cliquez sur **Ajouter un annuaire** et sélectionnez **Ajouter Active Directory via LDAP/IWA**.
- 4 Entrez les paramètres de compte Active Directory.

◆ Annuaires Active Directory non natifs

Option	Exemple d'entrée
Nom de l'annuaire	Saisissez un nom d'annuaire unique. Sélectionnez Active Directory via LDAP lorsque vous utilisez un annuaire Active Directory non natif.
Cet annuaire prendre en charge les services DNS	Désélectionnez cette option.
Nom unique de base	Entrez le nom unique (DN) du point de départ des recherches sur le serveur d'annuaire. Par exemple, cn=users,dc=rainpole,dc=local .
Nom unique de liaison	Entrez le nom unique (DN) complet, incluant le nom commun (CN), d'un compte d'utilisateur Active Directory qui dispose de privilèges de recherche d'utilisateurs. Par exemple, cn=config_admin infra,cn=users,dc=rainpole,dc=local .
Mot de passe du nom unique de liaison	Entrez le mot de passe Active Directory du compte autorisé à rechercher des utilisateurs.

◆ Annuaires Active Directory natifs

Option	Exemple d'entrée
Nom de l'annuaire	Saisissez un nom d'annuaire unique. Sélectionnez Active Directory (authentification Windows intégrée) lorsque vous utilisez Active Directory natif.
Nom de domaine	Entrez le nom du domaine à joindre.
Nom d'utilisateur de l'administrateur du domaine	Entrez le nom d'utilisateur de l'administrateur de domaine.
Mot de passe de l'administrateur du domaine	Entrez le mot de passe du compte de l'administrateur du domaine.
UPN de l'utilisateur Bind	Utilisez le format d'adresse électronique pour entrer le nom de l'utilisateur pouvant authentifier le domaine.
Mot de passe du nom unique de liaison	Entrez le mot de passe Bind Active Directory du compte autorisé à rechercher des utilisateurs.

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

6 Cliquez sur **Enregistrer et Suivant**.

La page **Sélectionner les domaines** s'ouvre et affiche la liste de domaines.

7 Acceptez le paramètre du domaine par défaut et cliquez sur **Suivant**.

8 Vérifiez que les noms d'attribut sont mappés sur les bons attributs d'Active Directory et cliquez sur **Suivant**.

9 Sélectionnez les groupes et les utilisateurs à synchroniser.

a Cliquez sur l'icône **Nouveau**.

b Entrez le domaine de l'utilisateur et cliquez sur **Rechercher des groupes**.

Par exemple, entrez **dc=vcac,dc=local**.

c Pour sélectionner les groupes à synchroniser, cliquez sur **Sélectionner**, puis sur **Suivant**.

d Sur la page **Sélectionner des utilisateurs**, sélectionnez les utilisateurs que vous souhaitez synchroniser et cliquez sur **Suivant**.

10 Vérifiez que les utilisateurs et les groupes se synchronisent avec l'annuaire et cliquez sur **Synchroniser avec l'annuaire**.

La synchronisation avec l'annuaire prend un certain temps et s'exécute en arrière-plan.

11 Sélectionnez **Administration > Gestion des annuaires > Fournisseurs d'identité**, puis cliquez sur le nouveau fournisseur d'identité.

Par exemple, **WorkspaceIDP__1**.

12 Faites défiler la page jusqu'au bas et mettez à jour la valeur pour que la propriété Nom d'hôte IdP pointe vers le nom de domaine complet de l'équilibrage de charge de vRealize Automation.

13 Cliquez sur **Enregistrer**.

14 Répétez les étapes 11 à 13 pour chaque locataire et fournisseur d'identité.

15 Après la mise à niveau de tous les nœuds vRealize Automation, connectez-vous à chaque locataire et sélectionnez **Administration > Gestion des annuaires > Fournisseurs d'identité**.

Tous les connecteurs vRealize Automation sont ajoutés à chaque fournisseur d'identité.

Par exemple, si votre déploiement comporte deux dispositifs vRealize Automation, deux connecteurs sont associés au fournisseur d'identité.

Migrer des groupes personnalisés vers l'instance cible de VMware Identity Manager

Vous devez migrer tous les groupes personnalisés de l'environnement source vers VMware Identity Manager (vIDM) dans le déploiement cible.

Effectuez cette procédure pour migrer les groupes personnalisés.

Conditions préalables

- [Créer un compte d'utilisateur local pour vos locataires](#).

- Assurez-vous que le service horizon-workspace est en cours d'exécution sur le dispositif virtuel vRealize Automation.

Procédure

- 1 Démarrez une session SSH sur le dispositif virtuel vRealize Automation.
- 2 À l'invite de commande, connectez-vous en tant qu'**utilisateur racine** avec le mot de passe que vous avez créé lorsque vous avez installé le dispositif virtuel vRealize Automation.
- 3 Exécutez cette commande.

```
vcac-config migrate-custom-groups
```

- Ce message s'affiche à la fin de la migration : La migration des groupes personnalisés s'est terminée correctement !
- Ce message s'affiche si votre environnement source ne contient aucun groupe personnalisé : Aucun groupe personnalisé n'a été trouvé dans la base de données vRA. Le processus de migration est ignoré.

Note Si une migration de groupe personnalisé échoue, affichez le fichier journal `/var/log/vmware/vcac/vcac-config.log` pour obtenir plus de détails.

Migrer plusieurs locataires et administrateurs IaaS

Pour chaque locataire vRealize Automation avec administrateurs de locataires ou administrateurs IaaS, vous devez supprimer et restaurer manuellement chaque administrateur.

Procédez comme suit pour chaque locataire dans la console vRealize Automation.


Conditions préalables

Connectez-vous à la console vRealize Automation sur le dispositif virtuel mis à niveau.

- 1 Ouvrez la console vRealize Automation sur le dispositif virtuel mis à niveau en utilisant son nom de domaine complet, `https://va-hostname.domain_name/vcac`.
Pour un environnement distribué, ouvrez la console sur le dispositif virtuel master.
- 2 Sélectionnez le domaine **vsphere.local**.
- 3 Connectez-vous avec le nom d'utilisateur **administrateur** et le mot de passe que vous avez entrés lors du déploiement du dispositif.

Procédure

- 1 Sélectionnez **Administration > Locataires**.
- 2 Cliquez sur le nom d'un locataire.
- 3 Cliquez sur **Administrateurs**.
- 4 Créez une liste des noms et noms d'utilisateur de chaque administrateur de locataires et administrateur IaaS.

- 5 Pointez chaque administrateur et cliquez sur l'icône de suppression  jusqu'à ce que vous ayez supprimé tous les administrateurs.
- 6 Cliquez sur **Terminer**.
- 7 Sur la page Locataires, cliquez de nouveau sur le nom du locataire.
- 8 Cliquez sur **Administrateurs**.
- 9 Entrez le nom de chaque utilisateur que vous avez supprimé dans la zone de recherche appropriée et appuyez sur Entrée.
- 10 Cliquez sur le nom de l'utilisateur approprié dans les résultats de la recherche pour rajouter l'utilisateur en tant qu'administrateur.

Lorsque vous avez terminé, la liste des administrateurs de locataires et des administrateurs IaaS ressemble à la liste des administrateurs que vous avez supprimée.

- 11 Cliquez sur **Terminer**.

Étape suivante

Mettez à niveau les dispositifs secondaires. Reportez-vous à [Installer la mise à jour sur des dispositifs vRealize Automation supplémentaires](#).

Installer la mise à jour sur des dispositifs vRealize Automation supplémentaires

Dans un environnement à haute disponibilité, le dispositif virtuel master est le nœud qui exécute la base de données PostgreSQL intégrée en mode master. Les autres nœuds de l'environnement exécutent la base de données PostgreSQL intégrée en mode réplica. Lors de la mise à niveau, le réplica d'un dispositif de réplica virtuel 6.2.5 ne requiert pas de modifications de la base de données.

Ne fermez pas l'interface de gestion du dispositif vRealize Automation pendant que vous installez la mise à jour.

Conditions préalables

- Vérifiez que vous avez téléchargé les mises à jour du dispositif virtuel. Reportez-vous à [Téléchargement des mises à jour du dispositif vRealize Automation](#).
- Vérifiez que la connexion de la base de données jdbc:postgresql pointe vers l'adresse IP externe du nœud master PostgreSQL.
 - a Sur le dispositif vRealize Automation, ouvrez une nouvelle invite de commandes.
 - b Accédez à `/etc/vcac/server.xml` et sauvegardez le fichier `server.xml`.
 - c Ouvrez le fichier `server.xml`.
 - d Si nécessaire, modifiez l'entrée du fichier `server.xml` `jdbc:postgresql` pour indiquer la base de données PostgreSQL que vous souhaitez utiliser.
 - Pour une base de données PostgreSQL externe, entrez l'adresse IP externe du nœud PostgreSQL master.

- Pour la base de données PostgreSQL intégrée, entrez l'adresse IP du dispositif virtuel master.

Par exemple, jdbc:postgresql://198.15.100.60:5432/vcac

Procédure

- 1 Ouvrez l'interface de gestion du dispositif vRealize Automation pour la mise à niveau.
 - a Connectez-vous en tant qu'utilisateur racine à chaque interface de gestion du dispositif vRealize Automation secondaire.

https://vrealize-automation-appliance-FQDN:5480
 - b Cliquez sur **Mise à jour**.
- 2 Cliquez sur **Paramètres**.
- 3 Sélectionnez pour télécharger les mises à jour depuis un référentiel VMware ou un CD-ROM dans la section Référentiel de mises à jour.
- 4 Cliquez sur **État**.
- 5 Cliquez sur **Vérifier les mises à jour** pour vérifier qu'une mise à jour est accessible.
- 6 Cliquez sur **Installer les mises à jour**.
- 7 Cliquez sur **OK**.

Un message indiquant que la mise à jour est en cours s'affiche.
- 8 (Facultatif) Si vous n'avez pas manuellement redimensionné Disque 1 Go à 50 Go, procédez comme suit.
 - a Lorsque le système vous invite à redémarrer le dispositif virtuel, cliquez sur **Système**, puis sur **Redémarrer**.

Pendant le redémarrage, le système ajuste l'espace requis sur Disque 1 pour la mise à jour.
 - b Après le redémarrage du système, déconnectez-vous, puis reconnectez-vous à l'interface de gestion du dispositif vRealize Automation et sélectionnez **Mettre à jour > État**.
 - c Cliquez sur **Vérifier les mises à jour** et **Installer les mises à jour**.
- 9 Pour vérifier que cette mise à niveau s'effectue correctement, ouvrez les fichiers journaux.
 - /opt/vmware/var/log/vami/vami.log
 - /opt/vmware/var/log/vami/updatecli.log
 - /var/log/vmware/horizon/horizon.log
 - /var/log/bootstrap/*.log

Pendant le processus de mise à niveau, si vous vous déconnectez et que vous vous reconnectez, vous pouvez continuer de suivre la progression de la mise à jour dans le fichier journal `/opt/vmware/var/log/vami/updatecli.log`.

Le temps nécessaire pour terminer la mise à jour dépend de votre environnement.

- 10** Lorsque la mise à jour est terminée, déconnectez-vous de l'interface de gestion du dispositif vRealize Automation, effacez le cache de votre navigateur Web et connectez-vous de nouveau à cette interface vRealize Automation.
- 11** Redémarrez le dispositif virtuel.
 - a Cliquez sur **Système**.
 - b Cliquez sur **Redémarrer** et confirmez votre sélection.
- 12** Une fois que le dispositif virtuel a redémarré, connectez-vous à l'interface de gestion du dispositif vRealize Automation du réplica.
- 13** Sélectionnez **Cluster**.
- 14** Entrez le nom d'utilisateur et le mot de passe du dispositif vRealize Automation master.
- 15** Cliquez sur **Joindre un cluster**.
- 16** Cliquez sur **Services** et vérifiez que tous les services, sauf `iaas-service`, sont répertoriés comme étant ENREGISTRÉS.

Étape suivante

[Mise à niveau des composants du serveur IaaS après la mise à niveau de vRealize Automation.](#)

Mise à niveau des composants du serveur IaaS après la mise à niveau de vRealize Automation

Après la mise à niveau de vRealize Automation 6.2.5, un administrateur système met à niveau les composants du serveur IaaS, notamment la base de données Microsoft SQL Server.

Vous avez deux options pour mettre à niveau les composants du serveur IaaS.

- Utilisez le script shell de mise à niveau d'IaaS automatisé.
- Utilisez le fichier exécutable du programme d'installation d'IaaS vRealize Automation fourni avec la version de vRealize Automation cible.

Si vous avez installé un composant du catalogue de composants communs, vous devez le désinstaller avant la mise à niveau. Après avoir terminé la mise à niveau, vous pouvez réinstaller le composant dans la version adéquate. Pour plus d'informations, reportez-vous au *Guide d'installation du catalogue de composants communs*. Si ce guide n'est pas disponible, utilisez la procédure de remplacement dans [Liste de contrôle pour la mise à niveau de vRealize Automation](#).

Mettre à niveau les composants IaaS à l'aide du script shell de mise à niveau

Utilisez le script shell de mise à niveau pour mettre à niveau les composants IaaS après la mise à jour de chaque dispositif vRealize Automation 6.2.5 vers la version de vRealize Automation cible.

Le dispositif vRealize Automation principal ou master mis à jour contient un script shell que vous utilisez pour mettre à niveau chaque nœud et composant IaaS.

Vous pouvez exécuter le script de mise à niveau à l'aide de la console vSphere pour la machine virtuelle ou à l'aide d'une session de console SSH. Si vous utilisez la console vSphere, vous évitez les problèmes de connectivité réseau intermittents qui peuvent interrompre l'exécution du script.

Si vous arrêtez le script pendant qu'il met à niveau un composant, le script s'exécute jusqu'à la fin de la mise à niveau sur le composant. Si un composant sur le nœud n'est pas mis à niveau, vous devez exécuter à nouveau le script.

Pour vérifier le résultat d'une mise à niveau, une fois terminée, ouvrez le fichier journal de mise à niveau dans `/usr/lib/vcac/tools/upgrade/upgrade.log`.

Conditions préalables

- Vérifiez l'aboutissement de la mise à niveau de tous les dispositifs vRealize Automation.
- Si vous redémarrez un serveur IaaS après avoir mis à jour tous les dispositifs vRealize Automation, vous devez arrêter les services IaaS Windows. Avant d'effectuer la mise à niveau des composants IaaS, arrêtez tous les services IaaS Windows, à l'exception du service Agent de gestion, sur le serveur.
- Avant d'exécuter le script shell de mise à niveau sur le nœud du dispositif vRealize Automation master ou principal, vérifiez que chaque service est ENREGISTRÉ.
 - a Connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.
`https://vrealize-automation-appliance-FQDN:5480`
 - b Cliquez sur **Services**.
 - c Vérifiez que tous les services, sauf iaas-service, sont ENREGISTRÉS.
- Mettez à niveau l'agent de gestion sur chaque machine virtuelle vRealize Automation IaaS.
 - a Dans un navigateur, ouvrez la page d'installation d'IaaS sur le dispositif vRealize Automation.
`https://vrealize-automation-appliance-FQDN:5480/installer`
 - b Cliquez sur **Programme d'installation de l'agent de gestion**.
Par défaut, le programme d'installation est téléchargé dans le dossier de téléchargement.
 - c Connectez-vous à chaque machine virtuelle vRealize Automation IaaS, mettez à niveau l'agent de gestion avec le fichier du **programme d'installation de l'agent de gestion**.

- Vérifiez que l'environnement d'exécution Java SE 8, 64 bits, Update 161 ou version ultérieure est installé sur le nœud du site Web IaaS sur lequel les données Model Manager sont installées. Après l'installation de Java, vous devez définir la variable d'environnement, JAVA_HOME, sur la nouvelle version.
 - Connectez-vous à chaque nœud de site Web IaaS et vérifiez que la date de création est antérieure à la date de modification dans le fichier `web.config`. Si la date de création du fichier `web.config` est identique ou ultérieure à la date de modification, suivez la procédure décrite dans [Échec de la mise à niveau pour le composant de site Web IaaS](#).
 - Pour vérifier que chaque nœud IaaS a un agent de gestion IaaS mis à niveau, appliquez la procédure suivante à chaque nœud IaaS.
 - a Connectez-vous à l'interface de gestion du dispositif vRealize Automation.
 - b Sélectionnez **Cluster**.
 - c Développez la liste de tous les composants installés sur chaque nœud IaaS, puis localisez l'agent de gestion IaaS.
 - d Vérifiez que la version de l'agent de gestion est à jour.
 - Vérifiez que la sauvegarde de la base de données IaaS Microsoft SQL Server est accessible au cas où vous devriez procéder à une restauration.
 - Supprimez tous les nœuds IaaS orphelins. Reportez-vous à [Supprimer les nœuds orphelins sur vRealize Automation](#).
 - Vérifiez que les snapshots des serveurs IaaS de votre déploiement sont disponibles.
- Si la mise à niveau échoue, revenez au snapshot et à la sauvegarde de la base de données, puis tentez une autre mise à niveau.

Procédure

- 1 Ouvrez une nouvelle session de console sur le nœud du dispositif vRealize Automation principal ou master et connectez-vous avec le compte racine.

Si vous prévoyez d'exécuter le script de mise à niveau au moyen de SSH, ouvrez une session de console SSH.
- 2 Passez au répertoire `/usr/lib/vcac/tools/upgrade/`.
- 3 À l'invite, exécutez cette commande pour créer le fichier `upgrade.properties`.

`./generate_properties`
- 4 Ouvrez le fichier `upgrade.properties` et entrez toutes les valeurs requises.

Ce tableau montre les valeurs requises, pouvant varier selon l'environnement. Par exemple, sur un nœud contenant un DEM Worker ou un DEM Orchestrator, les informations d'identification DEM sont requises.

Valeur requise	Description	Format des informations d'identification	Exemple de valeur
web_username	Nom d'utilisateur du nœud Web principal. Requis seulement une fois.	Domaine\Utilisateur	iaasDomain\webuser
web_password	Mot de passe du nœud Web principal. Requis seulement une fois.	Mot de passe	pa\$\$w0rd!
dem_username	Nom d'utilisateur du DEM Worker ou Orchestrator. Requis pour chaque nœud où un composant DEM est installé.	Domaine\Utilisateur	iaasDomain\demuser
dem_password	Mot de passe du DEM Worker ou Orchestrator. Requis pour chaque nœud où un composant DEM est installé.	Mot de passe	pa\$\$w0rd!
agent_username	Nom d'utilisateur pour un agent tel qu'un agent vSphere. Requis pour chaque nœud où un composant agent est installé.	Domaine\Utilisateur	iaasDomain\agent_user
agent_password	Mot de passe pour un agent tel qu'un agent vSphere. Requis pour chaque nœud où un composant agent est installé.	Mot de passe	pa\$\$w0rd!
vidm_admin_password	Mot de passe de l'administrateur VIDM. Requis uniquement lors d'une mise à niveau à partir de vRealize Automation 6.2.5.	VIDM_password	pa\$\$w0rd!

Pour des raisons de sécurité, le fichier `upgrade.properties` est supprimé lorsque vous exécutez le script shell de mise à niveau. Les propriétés du fichier sont définies à l'aide des informations de chaque composant IaaS qui est transmis via les agents de gestion IaaS. Il est important que tous les agents de gestion IaaS soient mis à niveau et dépourvus de défauts avant d'exécuter les scripts shell `./generate_properties` ou `./upgrade_from_62x`. Si un agent de gestion IaaS rencontre un problème lors de l'exécution du script shell de mise à niveau, reportez-vous à [La mise à jour ne réussit pas à mettre à jour l'agent de gestion](#). Pour recréer le fichier `upgrade.properties`, répétez les étapes 2 et 3.

5 Exécutez le script de mise à niveau.

- a À l'invite de commandes, entrez `./upgrade_from_62x`.
- b Appuyez sur Entrée.

Le script affiche chaque nœud IaaS et tous les composants qui y sont installés. Le script valide chaque composant avant l'installation de la mise à niveau. En présence de valeurs incorrectes dans le fichier `upgrade.properties`, le script échoue.

Le premier composant du serveur IaaS peut prendre 30 minutes ou plus. Pendant la mise à niveau, un message semblable à `Upgrading server components for node web1-vra.mycompany.com` s'affiche.

Si le script shell de mise à niveau échoue, vérifiez le fichier `upgrade.log`.

Vous pouvez réexécuter le script de mise à niveau après la correction d'un problème. Avant de réexécuter le script de mise à niveau, recréez le fichier `upgrade.properties`, ouvrez-le et entrez toutes les valeurs requises.

- 6 (Facultatif) Activez le basculement automatique de Manager Service. Reportez-vous à [Activer le basculement automatique de Manager Service après une mise à niveau](#).

Étape suivante

[Rétablir l'accès au centre de contrôle intégré de vRealize Orchestrator.](#)

Mise à niveau des composants IaaS à l'aide du programme d'installation d'IaaS

Vous pouvez utiliser cette autre méthode pour mettre à niveau les composants IaaS après la mise à niveau de vRealize Automation 6.2.5 vers la version de vRealize Automation cible.

Télécharger le programme d'installation de IaaS pour mettre à niveau les composants IaaS

Après la mise à niveau de vRealize Automation 6.2.5, téléchargez le programme d'installation d'IaaS sur la machine virtuelle où les composants IaaS devant être mis à niveau sont installés.

Si des avertissements de certificat s'affichent pendant cette procédure, vous pouvez les ignorer.

Note À l'exception d'une instance de sauvegarde passive du service du gestionnaire, le type de démarrage de tous les services doit être défini sur Automatique pendant le processus de mise à niveau. Si vous définissez des services sur Manuel, le processus de mise à niveau échoue.

Conditions préalables

- Vérifiez que Microsoft .NET Framework 4.5.2 ou une version ultérieure est installé sur la machine virtuelle d'installation d'IaaS. Vous pouvez télécharger le programme d'installation .NET à partir de la page d'installation de VMware vRealize Automation IaaS. Si vous mettez à jour .NET vers la version 4.5.2 après l'arrêt des services, la machine virtuelle peut redémarrer dans le cadre de l'installation. Dans ce cas, vous devez arrêter manuellement tous les services IaaS sur la machine virtuelle à l'exception de l'agent de gestion.
- Si vous utilisez Internet Explorer pour le téléchargement, vérifiez que l'option de configuration de sécurité renforcée n'est pas activée. Entrez `res://iesetup.dll/SoftAdmin.htm` dans la barre de recherche et appuyez sur Entrée.
- Connectez-vous en tant qu'administrateur local au serveur Windows sur lequel un ou plusieurs composants IaaS que vous voulez mettre à niveau sont installés.

Procédure

- 1 Dans un navigateur, ouvrez la page d'installation d'IaaS sur le dispositif vRealize Automation principal ou master.

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

- 2 Cliquez sur **Programme d'installation d'IaaS**.

- 3 Lorsque vous y êtes invité, enregistrez le fichier `setup__vrealize-automation-appliance-FQDN@5480.exe` sur le poste de travail.

Ne modifiez pas le nom du fichier. Le nom associe l'installation au dispositif vRealize Automation approprié.

Étape suivante

- Si vous disposez d'un cluster de dispositifs vRealize Orchestrator, reportez-vous à
- Reportez-vous à [Mettre à niveau les composants IaaS après la mise à niveau de vRealize Automation](#).

Mettre à niveau les composants IaaS après la mise à niveau de vRealize Automation

Après avoir effectué la mise à niveau à partir de vRealize Automation 6.2.5, vous devez mettre à niveau la base de données SQL et configurer tous les systèmes sur lesquels des composants IaaS sont installés. Vous pouvez suivre ces étapes pour les installations minimales et distribuées.

Note Le programme d'installation d'IaaS doit se trouver sur la machine virtuelle qui contient les composants IaaS que vous souhaitez mettre à niveau. Vous ne pouvez pas exécuter le programme d'installation depuis un emplacement externe, sauf pour la base de données Microsoft SQL qui peut également être mise à niveau à distance depuis le nœud Web.

Vérifiez que les snapshots des serveurs IaaS de votre déploiement sont disponibles. Si la mise à niveau échoue, vous pouvez revenir au snapshot et essayez une nouvelle fois de procéder à la mise à niveau.

Effectuez la mise à niveau afin que les services soient mis à niveau selon l'ordre suivant :

1 Sites Web IaaS

Si vous utilisez un équilibrage de charge, désactivez le trafic vers tous les nœuds non principaux.

Terminez la mise à niveau sur un serveur avant de réaliser la mise à niveau du prochain serveur exécutant un service de site Web. Commencez par celui sur lequel le composant Model Manager Data est installé.

Si vous effectuez une mise à niveau manuelle de la base de données Microsoft SQL externe, vous devez mettre à niveau la machine SQL externe avant de mettre à niveau le nœud Web. Vous pouvez mettre à niveau le SQL externe à distance à partir du nœud Web.

2 Manager Services

Mettez à niveau l'instance de Manager Service active avant de mettre à niveau l'instance de Manager Service passive.

Si vous n'avez pas activé le chiffrement SSL dans votre instance SQL, désélectionnez l'option **Chiffrement SSL** dans la boîte de dialogue de configuration de la mise à niveau d'IaaS.

3 DEM Orchestrator et DEM Workers

Mettez à niveau tous les DEM Orchestrator et les DEM Workers. Terminez la mise à niveau sur un serveur avant de réaliser la mise à niveau du prochain serveur.

4 Agents

Terminez la mise à niveau sur un serveur avant de réaliser la mise à niveau du prochain exécutant un agent.

5 Agent de gestion

Est mis à jour lors de la procédure de mise à niveau.

Si vous utilisez différents services sur un serveur, la mise à niveau met à jour les services dans le bon ordre. Par exemple, si le site Web et le composant Manager Service de votre site se trouvent sur le même serveur, veuillez les sélectionner les deux pour la mise à jour. Le programme d'installation de la mise à niveau effectue les mises à jour dans le bon ordre. Vous devez terminer la mise à niveau sur un serveur avant de commencer la mise à niveau d'un autre serveur.

Note Si votre déploiement utilise un équilibrage de charge, le premier dispositif que vous prévoyez de mettre à niveau doit être connecté à l'équilibrage de charge. Le trafic d'équilibrage de charge doit être désactivé pour toutes les autres instances de dispositif vRealize Automation avant que vous appliquiez la mise à niveau pour éviter les erreurs de mise en cache.

Conditions préalables

- Sauvegardez votre environnement vRealize Automation 6.2.5.
- Si vous redémarrez un serveur IaaS après avoir mis à jour tous les dispositifs vRealize Automation, vous devez arrêter les services IaaS Windows. Avant d'effectuer la mise à niveau des composants IaaS, arrêtez tous les services IaaS Windows, à l'exception du service Agent de gestion, sur le serveur.
- [Télécharger le programme d'installation de IaaS pour mettre à niveau les composants IaaS.](#)
- Assurez-vous que le nœud de site Web IaaS principal sur lequel les données Model Manager sont installées dispose de la bonne version de Java. L'environnement d'exécution JAVA SE 8, 64 bits, Update 161 ou version ultérieure doit être installé. Après l'installation de Java, définissez la variable d'environnement, JAVA_HOME, sur la nouvelle version.
- Vérifiez que la date de création est antérieure à la date de modification dans le fichier `web.config`. Si la date de création du fichier `web.config` est identique ou ultérieure à la date de modification, suivez la procédure décrite dans [Échec de la mise à niveau pour le composant de site Web IaaS](#).
- Si vous effectuez une mise à niveau à partir de vRealize Automation 6.2.5 et que vous utilisez une base de données Microsoft SQL externe, vous devez disposer de la bonne version de l'agent de gestion. L'agent de gestion sur la base de données externe doit être la version 7.0

ou version ultérieure avant qu'il soit possible d'exécuter la mise à niveau du site Web IaaS. Pour vérifier la version de l'agent de gestion, accédez au panneau de contrôle de votre machine virtuelle SQL externe. Si l'agent de gestion n'est pas la version 7.0 ou une version ultérieure, procédez comme suit pour mettre à niveau l'agent de gestion.

- a Dans un navigateur, accédez à la page d'installation d'IaaS.

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

- b Cliquez sur **Programme d'installation de l'agent de gestion**.

Par défaut, le programme d'installation est téléchargé dans le dossier de téléchargement.

- c Connectez-vous à la base de données externe, mettez l'agent de gestion à niveau avec le fichier du **programme d'installation de l'agent de gestion** et redémarrez le service de l'agent de gestion Windows.

- Si vous avez installé un composant du catalogue de composants communs, vous devez le désinstaller avant la mise à niveau. Pour plus d'informations, reportez-vous au *Guide d'installation du catalogue de composants communs* ou suivez les instructions fournies dans [Liste de contrôle pour la mise à niveau de vRealize Automation](#).

Procédure

- 1 Si vous utilisez un équilibrage de charge, préparez votre environnement.

- a Vérifiez que le nœud du site Web IaaS qui contient Model Manager Data est activé pour le trafic d'équilibrage de charge.

Vous pouvez identifier ce nœud par la présence du dossier `vCAC Folder\Server\ConfigTool`.

- b Désactivez tous les autres sites Web IaaS et le composant Manager Services non principal pour le trafic de l'équilibrage de charge.

- 2 Cliquez avec le bouton droit sur le fichier d'installation `setup__vrealize-automation-appliance-FQDN@5480.exe` et sélectionnez **Exécuter en tant qu'administrateur**.

- 3 Cliquez sur **Suivant**.

- 4 Acceptez le contrat de licence, puis cliquez sur **Suivant**.

- 5 Entrez les informations d'identification de l'administrateur pour le déploiement actif sur la page de connexion.

Le nom d'utilisateur est **root** et le mot de passe est celui que vous avez entré lorsque vous avez déployé le dispositif.

- 6 Sélectionnez **Accepter le certificat**.

- 7 Sur la page **Type d'installation**, vérifiez que **Mise à niveau** est sélectionné.

Si **Mise à niveau** n'est pas sélectionné, les composants de ce système sont déjà mis à niveau vers cette version.

- 8 Cliquez sur **Suivant**.

9 Configurez les paramètres de mise à niveau.

Option	Action
Si vous réalisez une mise à niveau de Model Manager Data	Sélectionnez la case Model Manager Data dans la section Serveur vCAC. La case est cochée par défaut. Effectuez la mise à niveau de Model Manager Data une seule fois. Lorsque vous mettez à niveau une installation distribuée, les serveurs Web cessent de fonctionner quand il y a une incompatibilité de version entre les serveurs Web et les données Model Manager. Lorsque la mise à niveau des données Model Manager est terminée, les serveurs Web fonctionnent comme d'habitude.
Si vous n'effectuez pas de mise à niveau de Model Manager Data	Désélectionnez la case Model Manager Data dans la section Serveur vCAC.
Pour conserver les workflows personnalisés à la dernière version dans votre Model Manager Data	Si vous mettez à niveau Model Manager Data, sélectionnez la case Conserver mes versions de workflow les plus récentes dans la section Workflows d'extensibilité. La case est cochée par défaut. Les workflows personnalisés sont toujours préservés. Le fait de sélectionner cette case détermine uniquement l'ordre des versions. Si vous avez personnalisé les workflows dans Model Manager, sélectionnez cette option afin que le workflow le plus récent reste considéré comme la version la plus récente après la mise à niveau. Si vous ne sélectionnez pas cette option, la version de chaque workflow fournie avec vRealize Automation Designer devient la plus récente après la mise à niveau et la version la plus récente avant la mise à niveau devient la deuxième. Pour plus d'informations sur vRealize Automation Designer, reportez-vous à <i>Extensibilité du cycle de vie</i> .
Si vous effectuez une mise à niveau d'un Distributed Execution Manager ou d'un agent de proxy	Saisissez les informations d'identification pour le compte d'administration dans la section Compte du service. Tous les services que vous mettez à niveau sont exécutés dans ce compte.
Pour spécifier votre base de données Microsoft SQL Server	Si vous mettez à niveau les données Model Manager, entrez les noms du serveur de base de données et de l'instance de base de données dans la zone de texte Serveur . Entrez un nom de domaine complet (FQDN) pour le nom de serveur de la base de données dans le champ de texte Nom de la base de données . Si l'instance de la base de données ne correspond pas à un port SQL par défaut, il vous faut inclure le numéro de port dans la spécification de l'instance de serveur. Le numéro de port Microsoft SQL par défaut est 1433. Lorsque vous mettez à niveau les nœuds du gestionnaire, l'option MSSQL SSL est sélectionnée par défaut. Si votre base de données n'utilise pas SSL, désélectionnez l'option Utiliser SSL pour la connexion à la base de données .

10 Cliquez sur **Suivant**.

11 Confirmez que tous les services à mettre à niveau s'affichent sur la page Prêt pour la mise à niveau, puis cliquez sur **Mettre à niveau**.

La page Mise à niveau et un indicateur de progression s'affichent. Lorsque la procédure de mise à niveau se termine, le bouton **Suivant** est activé.

12 Cliquez sur **Suivant**.

- 13 Cliquez sur **Terminer**.
- 14 Vérifiez que tous les services ont redémarré.
- 15 Répétez ces étapes pour chaque serveur IaaS de votre déploiement dans l'ordre indiqué.
- 16 Une fois tous les composants mis à niveau, connectez-vous à l'interface de gestion du dispositif vRealize Automation et vérifiez que tous les services, y compris IaaS, sont désormais enregistrés.

Résultats

Tous les composants sélectionnés sont mis à niveau vers la nouvelle version.

Étape suivante

- [Rétablir l'accès au centre de contrôle intégré de vRealize Orchestrator.](#)
- Si votre déploiement utilise un équilibrage de charge, mettez à niveau chaque nœud de l'équilibrage de charge pour utiliser les contrôles de santé vRealize Automation. Réactivez le trafic de l'équilibrage de charge pour tous les nœuds non connectés. Si votre précédent déploiement utilisait une base de données PostgreSQL intégrée faisant l'objet d'un équilibre de charge, désactivez tous les nœuds du pool PostgreSQL, car ils ne sont pas nécessaires. Supprimez le pool à un moment opportun.

Pour plus d'informations, reportez-vous à la partie *Équilibrage de charge de vRealize Automation*, dans la section *Documents d'équilibrage de charge* de la [documentation du produit vRealize Automation](#).
- (Facultatif) Activez le basculement automatique de Manager Service. Reportez-vous à [Activer le basculement automatique de Manager Service après une mise à niveau](#).

Rétablir l'accès au centre de contrôle intégré de vRealize Orchestrator

Après la mise à niveau des composants du serveur IaaS, vous devez restaurer l'accès à vRealize Orchestrator.

Lorsque vous procédez à la mise à niveau depuis vRealize Automation 6.2.5, vous devez effectuer cette procédure pour intégrer le contrôle d'accès basé sur les rôles. Cette procédure est disponible pour un environnement à haute disponibilité.

Conditions préalables

Prenez un snapshot de votre environnement vRealize Automation.

Procédure

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

`https://vrealize-automation-appliance-FQDN:5480`
- 2 Sélectionnez **Cluster**.
- 3 Identifiez les nœuds master et de réplica.

- 4 Sur chaque nœud de réplica, ouvrez une session SSH, connectez-vous en tant qu'administrateur et exécutez la commande suivante :

`service vco-server stop && service vco-configurator stop`
- 5 Sur le nœud master, ouvrez une session SSH, connectez-vous en tant qu'administrateur et exécutez la commande suivante :

`rm /etc/vco/app-server/vco-registration-id`
- 6 Sur le nœud master, passez au répertoire `/etc/vco/app-server /`.
- 7 Ouvrez le fichier `sso.properties`.
- 8 Si le nom de propriété `com.vmware.o11n.sso.admin.group.name` contient des espaces ou tout autre caractère Bash pouvant être accepté comme caractère spécial dans une commande Bash comme une apostrophe (') ou un symbole dollar (\$), procédez comme suit.
 - a Copiez la ligne incluant la propriété `com.vmware.o11n.sso.admin.group.name` et entrez `AdminGroup` pour la valeur.
 - b Ajoutez `#` au début de la ligne d'origine incluant la propriété `com.vmware.o11n.sso.admin.group.name` pour la mettre en commentaire.
 - c Enregistrez et fermez le fichier `sso.properties`.
- 9 Exécutez la commande suivante :

`vcac-vami vco-service-reconfigure`
- 10 Si vous avez effectué l'étape 8, ouvrez le fichier `sso.properties` et procédez comme suit.
 - a Supprimez le symbole `#` au début de la ligne d'origine incluant la propriété `com.vmware.o11n.sso.admin.group.name` pour annuler la mise en commentaire de la ligne.
 - b Supprimez la copie de la ligne incluant la propriété `com.vmware.o11n.sso.admin.group.name`.
 - c Enregistrez et fermez le fichier `sso.properties`.
- 11 Exécutez cette commande pour redémarrer le service `vco-server` :

`service vco-server restart`
- 12 Exécutez cette commande pour redémarrer le service `vco-configurator` :

`service vco-configurator restart`
- 13 Dans l'interface de gestion du dispositif vRealize Automation, cliquez sur **Services** et attendez que tous les services du nœud master soient ENREGISTRÉ.
- 14 Lorsque tous les services sont enregistrés, joignez les nœuds de réplica vRealize Automation au cluster vRealize Automation pour synchroniser la configuration de vRealize Orchestrator.

Étape suivante

[Migration d'une instance externe de vRealize Orchestrator après la mise à niveau de vRealize Automation.](#)

Migration d'une instance externe de vRealize Orchestrator après la mise à niveau de vRealize Automation

À partir de vRealize Orchestrator 7.5, vous ne pouvez plus mettre à niveau vos environnements vRealize Orchestrator externes. Pour mettre à niveau des environnements vRealize Orchestrator externes vers la dernière version, vous devez les migrer.

Note L'instance de vRealize Orchestrator intégrée dans vRealize Automation est automatiquement mise à niveau avec la mise à niveau de vRealize Automation. Si vous utilisez uniquement une instance intégrée de vRealize Orchestrator, aucune action n'est nécessaire.

La migration de vRealize Orchestrator transfère une configuration vRealize Orchestrator source externe vers votre environnement vRealize Orchestrator 7.5 récemment configuré. Tous les éléments existants, tels que les workflows, les actions, les éléments de configuration et de ressources, les modules, les tâches, les stratégies, les certificats, les plug-ins, etc., sont alors remplacés.

Il existe deux options pour la mise à niveau d'une instance externe de vRealize Orchestrator lorsque vous effectuez la migration vers la dernière version de vRealize Automation.

- Migrez votre instance externe de vRealize Orchestrator vers une autre instance externe de vRealize Orchestrator. Reportez-vous à [Migrer un serveur Orchestrator externe vers un environnement vRealize Orchestrator 7.5](#) dans la documentation de vRealize Orchestrator.
- Migrez votre serveur vRealize Orchestrator externe vers une instance intégrée de vRealize Orchestrator dans vRealize Automation. Reportez-vous à [Migrer un serveur Orchestrator externe vers un environnement vRealize Orchestrator 7.5](#) dans la documentation de vRealize Orchestrator.

Note La migration d'une instance intégrée de vRealize Orchestrator vers un environnement vRealize Orchestrator externe n'est pas prise en charge.

Ajouter des utilisateurs ou des groupes à une connexion Active Directory

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

Le système d'authentification des utilisateurs de la gestion des annuaires importe des données de l'annuaire Active Directory lors de l'ajout de groupes et d'utilisateurs. La vitesse du transport des données est limitée par les capacités d'Active Directory. Par conséquent, les actions peuvent être relativement longues selon le nombre de groupes et d'utilisateurs ajoutés. Afin de minimiser les problèmes, limitez les groupes et les utilisateurs aux groupes et utilisateurs requis pour une action vRealize Automation. En cas de problèmes, fermez les applications inutiles et vérifiez que votre déploiement alloue une capacité de mémoire adéquate à Active Directory. Si les problèmes persistent, augmentez l'allocation de mémoire Active Directory. Pour les déploiements comportant un nombre important d'utilisateurs et de groupes, vous devrez éventuellement allouer jusqu'à 24 Go de mémoire à Active Directory.

Lorsque vous synchronisez un déploiement vRealize Automation avec plusieurs utilisateurs et groupes, il peut y avoir un certain délai avant que les détails SyncLog deviennent disponibles. L'horodatage du fichier journal peut différer de l'heure d'achèvement indiquée sur la console.

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

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

Conditions préalables

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

Procédure

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

Pour modifier la configuration des groupes :

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

Pour modifier la configuration des utilisateurs :

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

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

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

Activer vos équilibres de charge

Si votre déploiement utilise des équilibres de charge, réactivez les nœuds secondaires et les contrôles de santé, puis rétablissez les paramètres de délai d'expiration d'équilibrage de charge.

Les contrôles de santé de vRealize Automation varient selon la version. Pour plus d'informations, reportez-vous au *Guide de Configuration de l'équilibrage de charge vRealize Automation* dans la documentation de [VMware vRealize Automation](#).

Rétablissez les paramètres de délai d'expiration d'équilibrage de charge de 10 minutes à la valeur par défaut.

Tâches à réaliser après la mise à niveau de vRealize Automation

Après la mise à niveau de vRealize Automation 6.2.5, effectuez toutes les tâches post-mise à niveau requises.

Configuration de port pour les déploiements à haute disponibilité

Après avoir terminé une mise à niveau dans un déploiement à haute disponibilité, il vous faut configurer l'équilibrage de charge pour faire passer le trafic du port 8444 vers le dispositif vRealize Automation pour prendre en charge les fonctionnalités de console distante.

Pour plus d'informations, reportez-vous au *Guide de configuration de l'équilibrage de charge de vRealize Automation* dans la [documentation de vRealize Automation](#).

Activation de l'action de connexion à la console distante pour les consommateurs

L'action de console distante pour les consommateurs est prise en charge pour les dispositifs provisionnés par vSphere dans vRealize Automation.

Modifier le Blueprint après avoir mis à niveau la version et sélectionnez l'action **Se connecter à la console distante** dans l'onglet **Action**.

Pour plus d'informations, reportez-vous à [l'article 2109706 de la base de connaissances](#).

Restaurer les fichiers de délai d'expiration du workflow externe

Vous devez reconfigurer les fichiers de délai d'expiration du workflow externe vRealize Automation, car la procédure de mise à niveau remplace les fichiers xmlldb.

Procédure

- 1 Ouvrez les fichiers configuration (xmldb) du workflow externe sur votre système dans l'annuaire suivant.

`\VMware\VCAC\Server\ExternalWorkflows\xmldb\.`
- 2 Remplacez les fichiers xmldb par les fichiers que vous avez sauvegardés avant la migration. Si vous n'avez pas de fichiers de sauvegarde, reconfigurez les paramètres de délai d'expiration du workflow externe.
- 3 Enregistrez vos paramètres.

Reconfigurer le point de terminaison d'infrastructure vRealize Orchestrator intégré dans le dispositif vRealize Automation cible

Lorsque vous migrez depuis un environnement vRealize Automation 6.2.5, vous devez mettre à jour l'URL du point de terminaison d'infrastructure qui pointe vers le serveur vRealize Orchestrator intégré cible.

Conditions préalables

- Migrez vers vRealize Automation vers la version de vRealize Automation cible.
- Connectez-vous à la console vRealize Automation cible.
 - a Ouvrez la console vRealize Automation à l'aide du nom de domaine complet du dispositif virtuel cible : `https://vra-vd-hostname.domain.name/vcac`.

 Pour un environnement à haute disponibilité, ouvrez la console à l'aide du nom de domaine complet de l'équilibrage de charge du dispositif virtuel cible : `https://vra-vd-lb-hostname.domain.name/vcac`.
 - b Connectez-vous en tant qu'utilisateur administrateur laaS.

Procédure

- 1 Sélectionnez **Infrastructure > Points de terminaison > Points de terminaison**.
- 2 Sur la page Points de terminaison, sélectionnez le point de terminaison vRealize Orchestrator, puis cliquez sur **Modifier**.
- 3 Dans la zone de texte Adresse, modifiez l'URL du point de terminaison vRealize Orchestrator.
 - Si vous avez migré vers un environnement minimal, remplacez l'URL du point de terminaison vRealize Orchestrator par `https://vra-vd-hostname.domain.name:443/vco`.
 - Si vous avez migré vers un environnement à haute disponibilité, remplacez l'URL du point de terminaison vRealize Orchestrator par `https://vra-vd-lb-hostname.domain.name:443/vco`.
- 4 Cliquez sur **OK**.

5 Exécutez manuellement une collecte de données sur le point de terminaison vRealize Orchestrator.

- a Sur la page Points de terminaison, sélectionnez le point de terminaison vRealize Orchestrator.
- b Sélectionnez **Actions > Collecte de données**.

Vérifiez que la collecte de données a réussi.

Modifier les scripts de workflow mis à niveau qui incluent des stratégies d'approbation

Si, dans vRealize Orchestrator 6.x, un script de workflow appelle des stratégies d'approbation vRealize Automation, vous devez modifier le script pour prendre en compte les modifications apportées dans vRealize Automation 7.0 et les versions ultérieures.

Au lieu d'appeler le service d'approbation pour qu'il appelle le client d'approbation, vous devez désormais appeler directement le client d'approbation.

Procédure

- 1 Si, dans vRealize Orchestrator 6.x, vous utilisez un script semblable à l'exemple suivant :

```
var service = vcacHost.createApprovalClient().getApprovalApprovalInfoService();
System.log( "got the service" );
var approvalInfo = service.getApprovalInfo( approvalId );
var approvalPolicy = approvalInfo.getPolicy();
```

- 2 Alors remplacez-le par un script semblable à cet exemple.

```
var approvalClient = vcacHost.createApprovalClient();

var vars = [
    approvalId
];

var approvalInfo = approvalClient.getWithVariables("/info/approvals/{0}", vars);
var approvalPolicy = new vCACCAFEApprovalDescriptiveReference() ;
approvalPolicy.setId(approvalInfo.getProperty("policy").getProperty("id"));
approvalPolicy.setName(approvalInfo.getProperty("policy").getProperty("name"));
approvalPolicy.setDescription(approvalInfo.getProperty("policy").getProperty("description"));
```

Restaurer les modifications apportées à la connexion dans le fichier app.config

Le processus de mise à niveau remplace les modifications que vous avez apportées à la connexion dans les fichiers de configuration. Après avoir procédé à une mise à niveau, vous devez restaurer toutes les modifications apportées au fichier app.config avant la mise à niveau.

Vous pouvez restaurer les modifications en effectuant une fusion sans remplacer les modifications apportées aux fichiers *.exe.config (par exemple, managervice.exe.config) sur votre serveur IaaS que vous avez sauvegardé lors des tâches prérequis.

Activer le basculement automatique de Manager Service après une mise à niveau

Le basculement automatique de Manager Service est désactivé par défaut lorsque vous effectuez une mise à niveau de vRealize Automation.

Appliquez cette procédure pour activer automatiquement Manager Service après la mise à niveau.

Procédure

- 1 Ouvrez une invite de commande en tant qu'utilisateur racine sur le dispositif vRealize Automation.
- 2 Changez les répertoires en `/usr/lib/vcac/tools/vami/commands`.
- 3 Pour activer le basculement automatique de Manager Service, exécutez la commande suivante.

```
python ./manager-service-automatic-failover ENABLE
```

Pour désactiver le basculement automatique dans un déploiement de IaaS, exécutez la commande suivante.

```
python ./manager-service-automatic-failover DISABLE
```

À propos du basculement automatique de Manager Service

Vous pouvez configurer Manager Service vRealize Automation IaaS pour basculer automatiquement sur une sauvegarde si l'instance principale de Manager Service s'arrête.

À partir de vRealize Automation 7.3, vous n'avez plus besoin de démarrer ou d'arrêter Manager Service manuellement sur chaque serveur Windows pour contrôler lequel est utilisé comme serveur principal ou de sauvegarde. Le basculement automatique de Manager Service est désactivé par défaut lorsque vous mettez à niveau IaaS à l'aide du script shell de mise à niveau ou du fichier exécutable du programme d'installation IaaS.

Lorsque le basculement automatique est activé, Manager Service démarre automatiquement sur tous les hôtes Manager Service, y compris les sauvegardes. La fonctionnalité de basculement automatique permet aux hôtes de se surveiller mutuellement de manière transparente et de basculer lorsque cela est nécessaire, mais le service Windows doit être en cours d'exécution sur tous les hôtes.

Note Vous n'êtes pas obligé d'utiliser le basculement automatique. Vous pouvez le désactiver et continuer de démarrer et d'arrêter manuellement le service Windows pour contrôler quel hôte sert d'hôte principal ou de sauvegarde. Si vous choisissez le basculement manuel, il vous suffit de démarrer le service sur un hôte à la fois. Avec le basculement automatique désactivé, l'exécution simultanée du service sur plusieurs serveurs IaaS rend vRealize Automation inutilisable.

Ne tentez pas d'activer ou de désactiver de manière sélective le basculement automatique. Le basculement automatique doit toujours être synchronisé, qu'il soit sous tension ou hors tension, sur chaque hôte Manager Service dans un déploiement IaaS.

Exécuter l'action Tester la connexion et vérifier les points de terminaison mis à niveau

La mise à niveau effectuée à partir de versions antérieures de vRealize Automation apporte des modifications à certains points de terminaison dans l'environnement cible.

Après la mise à niveau vers vRealize Automation, vous devez utiliser l'action **Tester la connexion** pour tous les points de terminaison applicables. Vous devrez également ajuster certains points de terminaison mis à niveau. Pour plus d'informations, reportez-vous à la section [Considérations lors de l'utilisation de points de terminaison mis à niveau ou migrés](#).

Le paramètre de sécurité par défaut pour les points de terminaison mis à niveau ou migrés consiste à ne pas accepter les certificats non approuvés.

Après la mise à niveau ou la migration à partir d'une version antérieure à vRealize Automation, si vous utilisez des certificats non approuvés, vous devez effectuer la procédure suivante pour tous les points de terminaison vSphere et NSX afin d'activer la validation du certificat. Si vous ne le faites pas, les opérations de point de terminaison échouent et produisent des erreurs de certificat. Pour plus d'informations, consultez les articles de la base de connaissances VMware *La communication au point de terminaison est interrompue après la mise à niveau vers vRA 7.3* (2150230) à l'adresse <http://kb.vmware.com/kb/2150230> et *Comment télécharger et installer des certificats vCenter Server racine pour éviter les avertissements de certificat de navigateur Web* (2108294) à l'adresse <http://kb.vmware.com/kb/2108294>.

- 1 Après une mise à niveau ou une migration, connectez-vous à la machine de l'agent vSphere/vRealize Automation et redémarrez vos agents vSphere à l'aide de l'onglet **Services**.
Il se peut que la migration ne fasse pas redémarrer tous les agents ; si tel est le cas, redémarrez-les manuellement.
- 2 Attendez qu'au moins un rapport de commande ping se termine. Cette opération peut prendre une à deux minutes.
- 3 Lorsque les agents vSphere ont démarré la collecte de données, connectez-vous à vRealize Automation en tant qu'administrateur laaS.
- 4 Cliquez sur **Infrastructure > Points de terminaison > Points de terminaison**.
- 5 Modifiez un point de terminaison vSphere et cliquez sur **Tester la connexion**.
- 6 Si une invite de certificat s'affiche, cliquez sur **OK** pour accepter le certificat.
Si aucune invite de certificat ne s'affiche, il se peut qu'actuellement le certificat soit correctement stocké dans une autorité racine approuvée du service d'hébergement de la machine Windows pour le point de terminaison, par exemple en tant que machine de l'agent proxy ou machine DEM.
- 7 Cliquez sur **OK** pour appliquer l'acceptation du certificat et enregistrer le point de terminaison.
- 8 Répétez cette procédure pour chaque point de terminaison vSphere.
- 9 Répétez cette procédure pour chaque point de terminaison NSX.

- 10 Accédez à **Infrastructure > Ressources de calcul**, cliquez avec le bouton droit sur votre ressource **vCenter Compute**, puis exécutez **Collecte de données**.

Si l'action **Tester la connexion** réussit, mais certaines opérations de collecte ou de provisionnement de données échouent, vous pouvez installer le même certificat sur toutes les machines de l'agent qui servent de point de terminaison et sur toutes les machines DEM. Vous pouvez également désinstaller le certificat des machines existantes et répéter la procédure précédente pour le point de terminaison défaillant.

Importer DynamicTypes

Si vous utilisez le plug-in DynamicTypes et que vous avez exporté la configuration sous la forme d'un module avant la mise à niveau, vous devez importer le workflow suivant :

- 1 Importez la configuration de DynamicTypes dans l'environnement cible.
 - a Connectez-vous à Java Client en tant qu'utilisateur administrateur.
 - b Sélectionnez l'onglet **Workflows**.
 - c Sélectionnez **Bibliothèque > Types dynamiques > Configuration**.
 - d Sélectionnez le workflow **Importer la configuration en tant que module** et exécutez-le.
 - e Cliquez sur **Module de configuration à importer**.
 - f Accédez au fichier de module exporté, puis cliquez sur **Joindre un fichier**.
 - g Passez en revue les informations sur les espaces de nommage joints au module et cliquez sur **Envoyer**.
- 2 Sélectionnez **Inventaire > Types dynamiques** pour vérifier que les espaces de noms de type dynamique ont été importés.

Résolution des problèmes de mise à niveau de vRealize Automation

Les rubriques de dépannage de mise à niveau offrent des solutions aux problèmes que vous pouvez rencontrer lors de la mise à niveau de vRealize Automation 6.2.5.

L'installation des mises à niveau échoue avec une erreur de délai d'attente des équilibrages de charge

Une installation ou une mise à niveau de vRealize Automation pour un déploiement distribué avec un équilibrage de charge échoue et renvoie une erreur de service 503 non disponible.

Problème

L'installation ou la mise à niveau échoue, car le paramètre d'expiration de l'équilibrage de charge n'accorde pas suffisamment de temps pour l'exécution de la tâche.

Cause

Un paramètre de délai d'expiration d'équilibrage de charge insuffisant peut entraîner un échec. Vous pouvez corriger le problème en augmentant le paramètre de délai d'expiration de l'équilibrage de charge à 100 secondes ou plus et en réexécutant la tâche.

Solution

- 1 Augmentez la valeur du délai d'expiration de l'équilibrage de charge à au moins 100 secondes.
- 2 Réexécutez l'installation ou la mise à niveau.

Échec de la mise à niveau pour le composant de site Web IaaS

La mise à niveau d'IaaS échoue et ne peut pas continuer.

Problème

La mise à niveau d'IaaS échoue pour le composant de site Web. Les messages d'erreur suivants s'affichent dans le fichier journal du programme d'installation.

- System.Data.Services.Client.DataServiceQueryException:
An error occurred while processing this request. --->
System.Data.Services.Client.DataServiceClientException: <!DOCTYPE html>
- **Description:** An application error
occurred on the server. The current custom error settings for this application prevent the details of the application error from being viewed remotely (for security reasons). It could, however, be viewed by browsers running on the local server machine.
- Warning: Non-zero return code. Command failed.
- Done Building Project "C:\Program Files
(x86)\VMware\VCAC\Server\Model Manager Data\DeployRepository.xml"
(InstallRepoModel target(s)) -- FAILED.

Les messages d'erreur suivants s'affichent dans le fichier journal de référentiel.

- [Error]: [sub-thread-Id="20"
context="" token=""] Failed to start repository service. Reason:
System.InvalidOperationException: Configuration section encryptionKey is not
protected
at
DynamicOps.Common.Utils.EncryptionHelpers.ReadKeyFromConfiguration(Configuration
config)
at DynamicOps.Common.Utils.EncryptionHelpers.Decrypt(String value)
at DynamicOps.Repository.Runtime.CoreModel.GlobalPropertyItem.Decrypt(Func`2
decryptFunc)

```

at
DynamicOps.Common.Entity.ContextHelpers.OnObjectMaterializedCallbackEncryptable(Object
t
sender, ObjectMaterializedEventArgs e)
at
System.Data.Common.Internal.Materialization.Shaper.RaiseMaterializedEvents()
at
System.Data.Common.Internal.Materialization.Shaper`1.SimpleEnumerator.MoveNext()
at System.Linq.Enumerable.FirstOrDefault[TSource](IEnumerable`1 source)
at System.Linq.Queryable.FirstOrDefault[TSource](IQueryable`1 source)
at
DynamicOps.Repository.Runtime.Common.GlobalPropertyHelper.GetGlobalPropertyItemValue(CoreModelEntities
coreModelContext, String propertyName, Boolean throwIfPropertyNotFound)
at
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.LoadSolutionUserCertificate()
at
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.InitializeFromDb(String
coreModelConnectionString)
at DynamicOps.Repository.Runtime.Common.RepositoryRuntime.Initialize().

```

Cause

La mise à niveau d'IaaS échoue lorsque la date de création du fichier `web.config` est identique ou ultérieure à la date de modification.

Solution

- 1 Sur l'hôte IaaS, connectez-vous à Windows.
- 2 Ouvrez l'invite de commande Windows.
- 3 Changez les répertoires pour le dossier d'installation de vRealize Automation.
- 4 Démarrez un éditeur de texte avec l'option **Exécuter en tant qu'administrateur**.
- 5 Localisez et sélectionnez le fichier `web.config` et enregistrez le fichier pour modifier sa date de modification.
- 6 Examinez les propriétés du fichier `web.config` afin de confirmer que la date de modification du fichier est postérieure à la date de création.
- 7 Mettez à niveau IaaS.

Manager Service échoue à s'exécuter en raison d'erreurs de validation du certificat SSL pendant l'exécution

Manager Service échoue à s'exécuter en raison d'erreurs de validation du certificat SSL.

Problème

Manager service échoue et renvoie le message d'erreur suivant dans le journal :

```
[Info] : Thread-Id="6" - context="" token="" Échec de la tentative de connexion à la
base de données principale. Nouvelle tentative dans 00:00:05. Détails de l'erreur :
une connexion a été établie avec le serveur, mais une erreur s'est ensuite produite
pendant le processus de connexion. (fournisseur : fournisseur SSL, erreur : 0 - La
chaîne de certificats a été émise par une autorité non autorisée.)
```

Cause

Pendant l'exécution, Manager Service échoue à s'exécuter en raison d'erreurs de validation du certificat SSL.

Solution

- 1 Ouvrez le fichier de configuration `ManagerService.config`.
- 2 Mettez à jour **Encrypt=False** à la ligne suivante :

```
<add name="vcac-repository" providerName="System.Data.SqlClient" connectionString="Data
Source=iaas-db.sqa.local;Initial Catalog=vcac;Integrated Security=True;Pooling=True;Max
Pool Size=200;MultipleActiveResultSets=True;Connect Timeout=200, Encrypt=True" />
```

La connexion échoue après une mise à niveau

Vous devez quitter le navigateur et vous reconnecter après une mise à niveau pour les sessions qui utilisent des comptes d'utilisateurs non synchronisés.

Problème

Après la mise à niveau de vRealize Automation, le système refuse de vous laisser accéder aux comptes d'utilisateurs non synchronisés lors de la connexion.

Solution

Quittez le navigateur et relancez vRealize Automation.

Des éléments de catalogue s'affichent dans le catalogue de services après la mise à niveau mais ne sont pas disponibles pour les demandes

Les éléments de catalogue qui utilisent certaines définitions de propriétés de versions précédentes figurent dans le catalogue de services, mais ne sont pas disponibles pour les demandes après la mise à niveau vers la dernière version de vRealize Automation.

Problème

Si vous avez procédé à la mise à niveau à partir de la version 6.2.x ou d'une version antérieure et que vous disposiez de définitions de propriétés avec les types de contrôle ou les attributs suivants, les attributs sont manquants dans les définitions de propriétés et les éléments de catalogue qui les utilisent ne fonctionnent plus comme avant la mise à niveau.

- Types de contrôle. Case à cocher ou lien.
- Attributs. Relation, expressions régulières ou dispositions de propriétés.

Cause

Dans vRealize Automation 7.0 et versions ultérieures, les définitions de propriétés n'utilisent plus les attributs. Vous devez créer à nouveau la définition de propriété ou la configurer de façon à utiliser une action de script vRealize Orchestrator au lieu des types de contrôle ou d'attribut intégrés.

Procédez à la migration des types de contrôle ou des attributs vers vRealize Automation 7 à l'aide d'une action de script.

Solution

- 1 Dans vRealize Orchestrator, créez une action de script qui renvoie les valeurs des propriétés. L'action doit renvoyer un type simple. Par exemple, des chaînes, des entiers ou d'autres types d'éléments pris en charge. L'action peut utiliser les autres propriétés dont elle dépend en tant que paramètre d'entrée.
- 2 Dans la console vRealize Automation, configurez la définition de produit.
 - a Sélectionnez **Administration > Dictionnaire des propriétés > Définitions de propriétés**.
 - b Sélectionnez la définition de propriété, puis cliquez sur **Modifier**.
 - c Dans le menu déroulant Afficher un conseil, sélectionnez **Liste déroulante**.
 - d Dans le menu déroulant Valeurs, sélectionnez **Valeurs externes**.
 - e Sélectionnez l'action de script.
 - f Cliquez sur **OK**.
 - g Configurez les paramètres d'entrée inclus dans l'action de script. Pour conserver la relation existante, liez le paramètre à l'autre propriété.
 - h Cliquez sur **OK**.

Échec de la fusion de la base de données PostgreSQL externe

La fusion de la base de données PostgreSQL externe avec la base de données PostgreSQL intégrée échoue.

Problème

Si la version de la base de données PostgreSQL externe est plus récente que celle de la base de données PostgreSQL intégrée, la fusion échoue.

Solution

1 Connectez-vous à l'hôte de la base de données PostgreSQL externe.

2 Exécutez la commande `psql --version`.

Notez la version de la base de données PostgreSQL externe.

3 Connectez-vous à l'hôte de la base de données PostgreSQL intégrée.

4 Exécutez la commande `psql --version`.

Notez la version de la base de données PostgreSQL intégrée.

Solution

Si la version de la base de données PostgreSQL externe est plus récente que celle de la base de données PostgreSQL intégrée, contactez le support pour obtenir de l'aide sur la fusion de votre base de données PostgreSQL externe.

La commande Joindre un cluster semble avoir échoué après la mise à niveau d'un environnement à haute disponibilité

Lorsque vous cliquez sur **Joindre un cluster** dans l'interface de gestion du dispositif vRealize Automation sur un nœud de cluster secondaire, l'indicateur de progression disparaît.

Problème

Lorsque vous utilisez l'interface de gestion du dispositif vRealize Automation après une mise à niveau pour joindre un nœud de cluster secondaire au nœud principal, l'indicateur de progression disparaît et aucun message d'erreur ou de réussite ne s'affiche. Ce comportement constitue un problème intermittent.

Cause

L'indicateur de progression disparaît, car certains navigateurs cessent d'attendre une réponse du serveur. Ce comportement n'arrête pas le processus de jonction du cluster. Vous pouvez vérifier que le processus de jonction du cluster est réussi en consultant le fichier journal dans `/var/log/vmware/vcac/vcac-config.log`.

La mise à niveau échoue si la partition racine ne fournit pas un espace libre suffisant

Si un espace libre suffisant n'est pas disponible sur la partition racine de l'hôte du dispositif vRealize Automation, la mise à niveau ne peut pas s'effectuer.

Cette procédure augmente l'espace libre sur la partition racine du disque 1 de l'hôte du dispositif vRealize Automation. Dans un déploiement distribué, effectuez cette procédure pour augmenter successivement l'espace libre sur chaque nœud de réplica, puis augmentez l'espace libre sur le nœud master.

Note Lorsque vous effectuez cette procédure, les messages d'avertissement suivants peuvent s'afficher :

- `WARNING: Re-reading the partition table failed with error 16:
Device or resource busy. The kernel still uses the old table. The
new table will be used at the next reboot or after you run
partprobe(8) or kpartx(8) Syncing disks.`
- `Error: Partition(s) 1 on /dev/sda have been written, but we have been unable to inform the kernel
of the change, probably because it/they are in use. As a result, the old partition(s) will remain
in use. You should reboot now before making further changes.`

Ignorez le message `Vous devez redémarrer maintenant avant d'apporter d'autres modifications`. Si vous redémarrez votre système avant l'étape 10, le processus de mise à niveau est compromis.

Solution

- 1 Mettez sous tension la machine virtuelle hôte du dispositif vRealize Automation et connectez-vous avec une connexion SSH (Secure Shell) en tant qu'utilisateur racine.
- 2 Exécutez les commandes suivantes pour arrêter les services.
 - a `service vcac-server stop`
 - b `service vco-server stop`
 - c `service vpostgres stop`
- 3 Exécutez la commande suivante pour démonter la partition d'échange.


```
swapoff -a
```
- 4 Exécutez la commande suivante pour supprimer les partitions Disque 1 existantes et pour créer une partition racine de 44 Go et une partition d'échange de 6 Go.


```
(echo d; echo 2; echo d; echo 1; echo n; echo p; echo ; echo ; echo '+44G'; echo  
n; echo p; echo ; echo ; echo ; echo w; echo p; echo q) | fdisk /dev/sda
```
- 5 Exécutez la commande suivante pour modifier le type de partition d'échange.


```
(echo t; echo 2; echo 82; echo w; echo p; echo q) | fdisk /dev/sda
```
- 6 Exécutez la commande suivante pour définir l'indicateur amorçable du disque 1.


```
(echo a; echo 1; echo w; echo p; echo q) | fdisk /dev/sda
```

- 7 Exécutez la commande suivante pour enregistrer les modifications de partition dans le noyau Linux.

```
partprobe
```

Si vous voyez un message vous invitant à redémarrer avant d'apporter d'autres modifications, ignorez ce message. Le redémarrage système avant l'étape 10 compromet le processus de mise à niveau.

- 8 Exécutez la commande suivante pour formater la nouvelle partition d'échange.

```
mkswap /dev/sda2
```

- 9 Exécutez la commande suivante pour monter la partition d'échange.

```
swapon -a
```

- 10 Redémarrez le dispositif vRealize Automation.

- 11 Après le redémarrage du dispositif, exécutez la commande suivante pour redimensionner la table de partition du disque 1.

```
resize2fs /dev/sda1
```

- 12 Pour vérifier que l'expansion du disque a réussi, exécutez `df -h` et vérifiez que l'espace disque disponible sur `/dev/sda1` est supérieur à 30 Go.

Copies de sauvegarde de fichiers .xml entraînant l'expiration du délai du système

vRealize Automation enregistre tous les fichiers possédant l'extension .xml dans le répertoire `\VMware\VCAC\Server\ExternalWorkflows\xmlldb\`. Si ce répertoire contient des fichiers de sauvegarde possédant l'extension .xml, le système exécute les workflows en double qui entraînent l'expiration du délai du système.

Solution : lorsque vous sauvegardez des fichiers dans ce répertoire, déplacez les sauvegardes dans un autre répertoire ou modifiez l'extension .xml dans le nom des fichiers.

Supprimer les nœuds orphelins sur vRealize Automation

Un nœud orphelin est un nœud dupliqué qui est signalé sur l'hôte mais n'y existe pas.

Problème

Lorsque vous vérifiez que chaque nœud IaaS et dispositif virtuel est sain, vous pouvez découvrir qu'un hôte comporte un ou plusieurs nœuds orphelins. Vous devez supprimer les nœuds orphelins.

Solution

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

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

- 2 Sélectionnez **Cluster**.

3 Pour chaque nœud orphelin dans le tableau, cliquez sur **Supprimer**.

Impossible de créer un nouveau répertoire dans vRealize Automation

Une tentative d'ajout d'un nouveau répertoire avec le premier connecteur de synchronisation échoue.

Problème

Cette erreur se produit en raison de la présence d'un fichier `config-state.json` incorrect dans `usr/local/horizon/conf/states/VSPHERE.LOCAL/3001/`.

Pour plus d'informations sur la correction de ce problème, reportez-vous à [l'article 2145438 de la base de connaissances](#).

Aucun déploiement n'est créé pour certaines machines virtuelles cours de la mise à niveau

Les machines virtuelles dont l'état indique qu'elles sont manquantes au moment de la mise à niveau n'ont pas de déploiement correspondant créé dans l'environnement cible.

Problème

Si une machine virtuelle est à l'état « manquant » dans l'environnement source pendant la mise à niveau, aucun déploiement correspondant n'est créé dans l'environnement cible. Si une machine virtuelle sort de l'état manquant après la mise à niveau, vous pouvez importer la machine dans le déploiement cible à l'aide d'une importation en bloc.

Erreur de certificat non approuvé

Lorsque vous affichez la page de la visionneuse du journal de l'infrastructure dans la console dispositif vRealize Automation, vous pouvez voir un rapport d'échec de connexion au point de terminaison avec le message : `Certificate is not trusted`.

Problème

Sur la console dispositif vRealize Automation, sélectionnez **Infrastructure > Surveillance > Journal**. Sur la page de la visionneuse du journal, vous pouvez voir un rapport semblable à celui-ci :

Échec de la connexion au point de terminaison. Pour confirmer que vous pouvez établir une connexion sécurisée à ce point de terminaison, accédez au point de terminaison vSphere sur la page Points de terminaison et cliquez sur le bouton Tester la connexion.

Exception interne : Certificat non approuvé (RemoteCertificateChainErrors). Objet : C=US, CN=vc6.mycompany.com Empreinte : DC5A8816231698F4C9013C42692B0AF93D7E35F1

Cause

La mise à niveau à partir de versions antérieures de vRealize Automation apporte des modifications aux points de terminaison depuis votre environnement d'origine. Après la mise à niveau de vRealize Automation, l'administrateur IaaS doit examiner chaque point de terminaison mis à niveau qui utilise une connexion https sécurisée. Si un point de terminaison renvoie une erreur `Certificate is not trusted`, le point de terminaison ne fonctionne pas correctement.

Solution

- 1 Connectez-vous à la console vRealize Automation en tant qu'administrateur de l'infrastructure.
- 2 Sélectionnez **Infrastructure > Points de terminaison > Points de terminaison**.
- 3 Procédez comme suit pour chaque point de terminaison ayant une connexion sécurisée.
 - a Cliquez sur **Modifier**.
 - b Cliquez sur **Tester la connexion**.
 - c Examinez les détails du certificat et cliquez sur **OK** si vous approuvez ce certificat.
 - d Redémarrez les services Windows pour tous les agents Proxy IaaS utilisés par ce point de terminaison.
- 4 Vérifiez que des erreurs `Certificate is not trusted` ne s'affichent plus sur la page de la visionneuse du journal d'infrastructure.

L'installation ou la mise à niveau vers vRealize Automation échoue lors de l'application des correctifs requis

L'installation ou la mise à niveau vers vRealize Automation échoue et un message d'erreur figure dans le fichier journal.

Problème

Lorsque vous procédez à l'installation ou à la mise à niveau vers vRealize Automation, la procédure échoue. Cela se produit généralement lorsque l'application d'un correctif au cours de l'installation ou de la mise à niveau échoue. Un message d'erreur figure dans le fichier journal semblable au message suivant : `Security error. Applying automatic fix for FIREWALL prerequisite failed. RPM Status 1: Pre install script failed, package test and installation skipped.`

Cause

Dans l'environnement Windows, une stratégie de groupe pour l'exécution du script PowerShell est définie sur `Activé`.

Solution

- 1 Sur la machine hôte Windows, exécutez `gpedit.msc` pour ouvrir l'éditeur de stratégie de groupe locale.

- 2 Dans le volet de gauche sous **Configuration ordinateur**, cliquez sur le bouton Développer pour ouvrir **Modèles d'administration > Composants Windows > Windows PowerShell**.
- 3 Pour **Activer l'exécution des scripts**, remplacez l'état Enabled par Not Configured.

La mise à jour ne réussit pas à mettre à jour l'agent de gestion

Un message d'erreur sur l'agent de gestion s'affiche lorsque vous cliquez sur **Installer les mises à jour** sur la page d'état de mise à jour de l'interface de gestion du dispositif vRealize Automation.

Problème

Le processus de mise à niveau a échoué. Un message s'affiche : Impossible de mettre à niveau l'agent de gestion sur le nœud x. Parfois ce message mentionne plusieurs nœuds.

Cause

De nombreuses conditions peuvent provoquer ce problème. Le message d'erreur identifie uniquement l'ID du nœud de la machine concernée. Vous trouverez plus d'informations dans le fichier ALL.log pour l'agent de gestion sur la machine où la commande a échoué.

Effectuez ces tâches sur les nœuds concernés selon votre situation :

Solution

- ◆ Si le service de l'agent de gestion n'est pas en cours d'exécution, démarrez le service et relancez la mise à niveau sur le dispositif virtuel.
- ◆ Si le service de l'agent de gestion est en cours d'exécution et que l'agent de gestion est mis à niveau, redémarrez la mise à niveau sur le dispositif virtuel.
- ◆ Si le service de l'agent de gestion est en cours d'exécution, mais que l'agent de gestion n'est pas mis à niveau, procédez à une mise à niveau manuelle.
 - a Dans le navigateur, accédez à la page d'installation d'laaS.
<https://vrealize-automation-appliance-FQDN:5480/installer>
 - b Téléchargez et exécutez le programme d'installation de l'agent de gestion.
 - c Redémarrez la machine de l'agent de gestion.
 - d Redémarrez la mise à niveau sur le dispositif virtuel.

La mise à niveau de l'agent de gestion a échoué

La mise à niveau de l'agent de gestion a échoué pendant la mise à niveau de vRealize Automation.

Problème

Si un incident de basculement a permuté l'hôte de l'agent de gestion principal et secondaire, la mise à niveau échoue, car le processus de mise à niveau automatisé ne peut pas trouver l'hôte attendu. Effectuez cette procédure sur chaque nœud laaS sur lequel l'agent de gestion n'est pas mis à niveau.

Solution

- 1 Ouvrez le fichier All.log dans le dossier des journaux de l'agent de gestion, qui se trouve dans C:\Program Files (x86)\VMware\VCAC\Management Agent\Logs\.

L'emplacement du dossier d'installation peut être différent de l'emplacement par défaut.

- 2 Recherchez dans le fichier journal un message sur un dispositif virtuel obsolète ou hors tension.

Par exemple, EXCEPTION INTERNE : System.Net.WebException : Impossible de se connecter au serveur distant ---> System.Net.Sockets.SocketException: Une tentative de connexion a échoué, car le participant connecté n'a pas répondu convenablement au-delà d'une certaine durée, ou une connexion établie a échoué car l'hôte de connexion n'a pas répondu *IP_Address:5480*

- 3 Modifiez le fichier de configuration de l'agent de gestion dans C:\Program Files (x86)\VMware\VCAC\Management Agent\VMware.IaaS.Management.Agent.exe.config pour remplacer la valeur alternativeEndpointaddress existante par l'URL du point de terminaison du dispositif virtuel principal.

L'emplacement du dossier d'installation peut être différent de l'emplacement par défaut.

Exemple de valeur alternativeEndpointaddress dans

VMware.IaaS.Management.Agent.exe.config.

```
<alternativeEndpoint address="https://FQDN:5480/" thumbprint="thumbprint number" />
```

- 4 Redémarrez le service de l'agent de gestion Windows et vérifiez le fonctionnement du fichier All.log.
- 5 Exécutez la procédure de mise à niveau sur le dispositif vRealize Automation principal.

Échec de la mise à jour de vRealize Automation en raison des paramètres de délai d'expiration par défaut

Vous pouvez augmenter le paramètre de temporisation pour la mise à jour si le paramètre par défaut pour la synchronisation des bases de données est trop court pour votre environnement.

Problème

Le paramètre de délai d'expiration pour la commande Vcac-Config SynchronizeDatabases n'est pas suffisant pour certains environnements où la synchronisation des bases de données est plus longue que la valeur par défaut de 3 600 secondes.

Les valeurs des propriétés `cafeTimeoutInSeconds` et `cafeRequestPageSize` dans le fichier `Vcac-Config.exe.config` régissent la communication entre l'API et l'utilitaire `Vcac-config.exe`. Le fichier se trouve à *l'emplacement d'installation d'IaaS\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe.config*.

Vous pouvez remplacer la valeur de délai d'expiration par défaut uniquement pour la commande `SynchronizeDatabases` en fournissant une valeur pour ces paramètres facultatifs.

Paramètre	Nom court	Description
--DatabaseSyncTimeout	-dstm	Définit la valeur de délai d'expiration de demande HTTP uniquement pour SynchronizeDatabases en secondes.
--DatabaseSyncPageSize	-dsps	Définit la taille de page de demande de synchronisation uniquement pour la synchronisation de réservation ou de stratégie de réservation. La valeur par défaut est 10.

Si ces paramètres ne sont pas définis dans le fichier `Vcac-Config.exe.config`, le système utilise le délai d'expiration par défaut.

Échec de la mise à niveau d'IaaS dans un environnement haute disponibilité

Échec du processus de mise à niveau d'IaaS sur le nœud du serveur Web principal sur lequel l'équilibrage de charge est activé. Vous pouvez voir ces messages d'erreur :

« System.Net.WebException : L'opération a expiré » ou « 401 - Non autorisé : L'accès est refusé en raison d'informations d'identification non valides. »

Problème

La mise à niveau d'IaaS lorsque l'équilibrage de charge est activé peut provoquer un échec intermittent. Dans ce cas, vous devez réexécuter la mise à niveau de vRealize Automation en désactivant l'équilibrage de charge au préalable.

Solution

- 1 Restaurez votre environnement aux snapshots antérieurs à la mise à jour.
- 2 Ouvrez une connexion Bureau à distance au nœud de serveur Web IaaS principal.
- 3 Accédez au fichier d'hôtes Windows dans `c:\windows\system32\drivers\etc`.
- 4 Ouvrez le fichier d'hôtes et ajoutez cette ligne pour qu'il contourne l'équilibrage de charge du serveur Web.

IP_address_of_primary_iaas_website_node vrealizeautomation_iaas_website_lb_fqdn

Exemple :

10.10.10.5 vra-iaas-web-lb.domain.com

- 5 Enregistrez le fichier d'hôtes et réessayez la mise à jour de vRealize Automation.
- 6 À la fin de la mise à jour de vRealize Automation, ouvrez le fichier d'hôtes et supprimez la ligne que vous avez ajoutée à l'étape 4.

Stockage différé après la mise à niveau

Les stockages ne s'affichent pas sous l'onglet Réservation.

Si les stockages ne s'affichent pas dans l'onglet Réservations après la mise à niveau, un redémarrage de vcac-server est requis sur tous les nœuds. L'affichage des stockages peut prendre jusqu'à une heure dans la section des ressources sous l'onglet Réservations.

Résoudre les problèmes de mise à niveau

Vous pouvez modifier le processus de mise à niveau pour résoudre les problèmes associés.

Lorsque vous rencontrez des problèmes de mise à niveau de votre environnement vRealize Automation, utilisez cette procédure pour modifier le processus de mise à niveau en sélectionnant l'un des indicateurs disponibles.

Solution

- 1 Ouvrez une connexion Secure Shell (SSH) au nœud du dispositif vRealize Automation principal.
- 2 À l'invite de commandes, exécutez cette commande pour créer le fichier de basculement :

`touch available_flag`

Par exemple : **`touch /tmp/disable-iaas-upgrade`**

Tableau 1-70. Indicateurs disponibles

Indicateur	Description
<code>/tmp/disable-iaas-upgrade</code>	<ul style="list-style-type: none"> ■ Empêche le processus de mise à niveau d'laaS après le redémarrage du dispositif virtuel. ■ Empêche la mise à niveau de l'agent de gestion. ■ Empêche les vérifications et les correctifs automatiques de conditions préalables. ■ Empêche l'arrêt des services laaS.
<code>/tmp/do-not-upgrade-ma</code>	Empêche la mise à niveau de l'agent de gestion. Cet indicateur est approprié lorsque l'agent de gestion est mis à niveau manuellement.
<code>/tmp/skip-prereq-checks</code>	Empêche les vérifications et les correctifs automatiques de conditions préalables. Cet indicateur est approprié lorsqu'il existe un problème lié aux correctifs automatiques de conditions préalables et que ceux-ci ont dû être appliqués manuellement.
<code>/tmp/do-not-stop-services</code>	Empêche l'arrêt des services laaS. La mise à niveau n'arrête pas les services Windows laaS tels que le service de gestion, les DEM et les agents.
<code>/tmp/do-not-upgrade-servers</code>	<p>Empêche la mise à niveau automatique de tous les composants Server laaS tels que la base de données, le site Web, WAPI, le référentiel, les données de modèle Mfrontanager et le service de gestion.</p> <p>Note Cet indicateur empêche également l'activation du mode de basculement automatique du service de gestion.</p>

Tableau 1-70. Indicateurs disponibles (suite)

Indicateur	Description
/tmp/do-not-upgrade-dems	Empêche la mise à niveau de DEM.
/tmp/do-not-upgrade-agents	Empêche la mise à niveau de l'agent proxy IaaS.

3 Effectuez les tâches correspondant à l'indicateur choisi.

Tableau 1-71. Tâches supplémentaires

Indicateur	Tâches
/tmp/disable-iaas-upgrade	<ul style="list-style-type: none"> ■ Mettez à niveau manuellement l'agent de gestion. ■ Appliquez manuellement toutes les conditions préalables IaaS requises. ■ Arrêtez manuellement les services IaaS. <ol style="list-style-type: none"> a Connectez-vous à votre serveur Windows IaaS. b Sélectionnez Démarrer > Outils d'administration > Services. c Arrêtez ces services dans l'ordre suivant. <p>Note N'arrêtez pas le serveur Windows IaaS.</p> <ol style="list-style-type: none"> a Chaque agent proxy VMwarevRealize Automation. b Chaque VMware DEM Worker. c VMware DEM Orchestrator. d Le service VMware vCloud Automation Center. ■ Démarrez manuellement la mise à niveau d'IaaS après celle du dispositif virtuel.
/tmp/do-not-upgrade-ma	Mettez à niveau manuellement l'agent de gestion.
/tmp/skip-prereq-checks	Appliquez manuellement toutes les conditions préalables IaaS requises.
/tmp/do-not-stop-services	<p>Arrêtez manuellement les services IaaS.</p> <ol style="list-style-type: none"> 1 Connectez-vous à votre serveur Windows IaaS. 2 Sélectionnez Démarrer > Outils d'administration > Services. 3 Arrêtez ces services dans l'ordre suivant. <p>Note N'arrêtez pas le serveur Windows IaaS.</p> <ol style="list-style-type: none"> a Chaque agent proxy VMwarevRealize Automation. b Chaque VMware DEM Worker. c VMware DEM Orchestrator. d Le service VMware vCloud Automation Center.
/tmp/do-not-upgrade-servers	

Tableau 1-71. Tâches supplémentaires (suite)

Indicateur	Tâches
/tmp/do-not-upgrade-dems	
/tmp/do-not-upgrade-agents	

- 4 Accédez à la console de gestion du dispositif vRealize Automation et mettez à jour le dispositif vRealize Automation principal.

Note Étant donné que chaque indicateur reste actif jusqu'à ce qu'il soit supprimé, exécutez cette commande pour supprimer l'indicateur choisi après la mise à niveau :

rm /flag_path/flag_name. Par exemple, **rm /tmp/disable-iaas-upgrade.**

Échec de la mise à niveau du dispositif virtuel lors de la vérification des conditions préalables IaaS

La vérification des conditions préalables IaaS ne parvient pas à valider les environnements configurés avec un nom de site Web IIS personnalisé. La désactivation de la mise à niveau d'IaaS automatisée corrige le problème.

Problème

La mise à niveau du dispositif virtuel échoue lors de la vérification des conditions préalables IaaS lors de l'exécution de scripts de préinstallation et de scripts de post-installation.

Error: Unrecognized configuration path MACHINE/WEBROOT/APPHOST/Default Web Site can not find path IIS:\Sites\Default Web Site because it does not exist.

Lorsque l'échec se produit, un message d'erreur similaire au message suivant s'affiche : Applying automatic fix for <prerequisite check name> prerequisite failed.

Cause

La vérification des conditions préalables IaaS ne parvient pas à valider les environnements configurés avec un nom de site Web IIS personnalisé. La désactivation des vérifications des conditions préalables automatisées de mise à niveau d'IaaS corrige le problème.

Solution

- 1 Désactivez les vérifications et correctifs des conditions préalables automatisées de mise à niveau d'IaaS.
- 2 Procédez à la mise à niveau de vRealize Automation. Consultez [Résoudre les problèmes de mise à niveau](#).

- 3 Suivez les invites de mise à niveau. Lorsque les invites vous dirigent à redémarrer vRealize Automation, vous pouvez utiliser le programme d'installation d'laaS pour rechercher les conditions préalables laaS non satisfaites et les corriger manuellement.

Note Ne redémarrez pas le dispositif tant que vous n'avez pas terminé la validation des conditions préalables laaS.

- 4 Utilisez les étapes suivantes pour chaque nœud de site Web laaS.
 - a Téléchargez le programme d'installation d'laaS. Consultez [Télécharger le programme d'installation d'laaS pour mettre à niveau les composants laaS après la mise à niveau du dispositif vRealize Automation](#).
 - b La première fois que vous initialisez le programme d'installation d'laaS, il génère un nouveau fichier de configuration sous le même répertoire avec l'extension `.exe.config`.
 - c Fermez le programme d'installation d'laaS et ajoutez la clé suivante dans la section `<appSettings>` du fichier de configuration. La clé transmet le nom de votre site Web personnalisé à l'outil de vérification des conditions préalables laaS.


```
<add key="PreReqChecker.Default.DefaultWebSite" value="custom_web_site_name"/>
```
 - d Enregistrez le fichier de configuration et relancez le programme d'installation d'laaS. Suivez les instructions à l'écran, jusqu'à ce que la validation des conditions préalables soit terminée. Si des conditions préalables ont été importées, corrigez-les manuellement.
- 5 Activez la mise à niveau automatique d'laaS en fermant le programme d'installation d'laaS et en redémarrant le dispositif vRealize Automation mis à niveau.

Note Si vous décidez de continuer manuellement la mise à niveau d'laaS à l'aide du programme d'installation d'laaS, redémarrez d'abord le dispositif vRealize Automation mis à niveau et attendez que tous les services soient enregistrés. Il vous faut mettre à niveau et configurer tous les systèmes qui possèdent des composants laaS. Pour plus d'informations, reportez-vous à la section [Mettre à niveau les composants laaS après la mise à niveau de vRealize Automation vers la version cible](#).

Migration de vRealize Automation

Vous pouvez effectuer une mise à niveau en parallèle de votre environnement vRealize Automation actuel vers la version la plus récente de vRealize Automation à l'aide de la migration.

Ces informations sont spécifiques à la mise à niveau de vRealize Automation vers la version 7.5 à l'aide de la migration. Pour plus d'informations sur les autres chemins de mise à niveau pris en charge, reportez-vous à *Mise à niveau depuis vRealize Automation 6.2.5* ou *Mise à niveau depuis vRealize Automation 7.1* ou version ultérieure dans la [documentation du produit vRealize Automation](#).

Migration de vRealize Automation

Vous pouvez effectuer une mise à niveau en parallèle de votre environnement vRealize Automation actuel à l'aide de la migration.

La migration déplace toutes les données, à l'exception des locataires et des magasins d'identités, de votre environnement vRealize Automation source actuel vers un déploiement cible de la dernière version de vRealize Automation. En outre, la migration déplace toutes les données de l'instance de vRealize Orchestrator 7.x intégrée vers le déploiement cible.

La migration ne modifie pas votre environnement source à l'exception de l'arrêt des services vRealize Automation pendant la période requise pour collecter et copier les données en toute sécurité vers votre environnement cible. Selon la taille de la base de données vRealize Automation source, la migration peut prendre de quelques minutes à plusieurs heures.

Vous pouvez migrer votre environnement source vers un déploiement minimal ou un déploiement haute disponibilité.

Si vous prévoyez de mettre votre environnement cible en production après la migration, ne remettez pas votre environnement source en service. Les modifications apportées à votre environnement source après la migration ne sont pas synchronisées avec votre environnement cible.

Si votre environnement source est intégré à vCloud Air ou vCloud Director, ou s'il dispose de points de terminaison physiques, vous devez utiliser la migration pour effectuer une mise à niveau. La migration supprime de l'environnement cible ces points de terminaison, ainsi que tout ce qui leur est associé. La migration supprime également l'intégration de VMware vRealize Application Services qui était prise en charge dans vRealize Automation 6.2.5.

Note Vous devez effectuer des tâches supplémentaires pour préparer vos machines virtuelles vRealize Automation avant de migrer. Avant de procéder à la migration, consultez l'article [51531](#) de la base de connaissances.

Si vous migrez depuis vRealize Automation 6.2.5, vous pouvez rencontrer des problèmes. Pour plus d'informations, reportez-vous à [Scénarios de migration](#).

Liste de contrôle de migration

Utilisez cette liste de contrôle pour suivre votre travail avant, pendant et après la migration de vRealize Automation.

Note Exécutez un [Exécutez un test de migration](#) avant une migration de production pour tester les cas d'utilisation de provisionnement et signalez tout problème pouvant survenir lors de la migration.

Tableau 1-72. Pré-migration

Étape	Référence
Déployer une installation de vRealize Automation	Consultez le Utilisation de l'assistant d'installation pour les déploiements d'entreprise de vRealize Automation.
Sauvegarder votre installation actuelle	Pour plus d'informations sur la sauvegarde et la restauration de votre système, reportez-vous à Sauvegarder votre environnement vRealize Automation 6.2.5 existant . Pour obtenir des informations générales, reportez-vous à la section Configuration de la sauvegarde et de la restauration à l'aide de Symantec NetBackup
Valider toutes les conditions préalables	Reportez-vous à la section Conditions préalables à la migration .
Préparer la cible avec des tâches préalables à la migration	Reportez-vous à la section Tâches préalables à la migration .
Exécuter un test de migration	Reportez-vous à la section Exécutez un test de migration .

Tableau 1-73. Migration

Étape	Référence
Exécuter une migration	Une fois que le test de migration a été vérifié et réussi, exécutez votre migration de production conformément à ces Procédures de migration .

Tableau 1-74. Post-migration

Étape	Référence
Tâches de post-migration	Effectuez les Tâches post-migration lorsque la migration est terminée.
Valider l'environnement migré	Reportez-vous à la section Valider l'environnement vRealize Automation cible .
Migration pour la vérification du scénario 6.2.x	Si vous migrez de la version 6.2 à la version 7.x, vérifiez les Scénarios de migration afin d'identifier les différences.

Exécutez un test de migration

Il est essentiel d'exécuter un test de migration pour valider les cas d'utilisation de provisionnement avant de migrer votre environnement de production. Tester une migration est nécessaire pour remodeler les Blueprints, workflows ou scripts qui peuvent avoir changé en raison des améliorations de la conception dans les versions ultérieures. Pour éviter des modifications non souhaitées aux charges de travail gérées, les administrateurs vRealize Automation doivent être vigilants lors du test.

Procédure

- 1 Déployez une installation minimale de vRealize Automation.

- 2 Définissez les éléments suivants sur la cible lorsque la migration se termine :
 - a Arrêtez les agents proxy et interrompez les notifications par e-mail après la migration.
 - b Annulez l'enregistrement des charges de travail en raison de l'expiration ou de l'allongement du bail.
 - c Définissez les agents proxy DoDeletes sur `false` sur la cible. Si votre événement expire, la cible ne détruit pas votre charge de travail.
 - d Faites correspondre le système source en surveillant les baux dans le système cible. Empêchez que le système expire en gardant les baux synchronisés.
 - e Supprimez des profils réseau de la réservation si vous prévoyez de tester le provisionnement et d'utiliser des fichiers réseau. La suppression des fichiers empêche la duplication d'adresses IP sur la source et la cible.
- 3 Exécutez un test de migration pour vRealize Orchestrator et vRealize Automation.
- 4 Validez et comparez l'environnement source avec la cible. Identifiez des zones où des modifications sont nécessaires.
- 5 Consultez les sorties de l'outil d'aide à la mise à niveau de test de production vRealize lors de la migration depuis la version 6.2.x vers la dernière version. L'outil identifie à quel endroit des améliorations dans vos workflows sont nécessaires.

Pour plus d'informations sur l'outil, reportez-vous à la section *Test de production vRealize Automation* dans la [documentation du produit vRealize Automation](#).
- 6 Enregistrez et conservez les informations et workflows modifiés afin de pouvoir les importer et les transférer facilement vers la migration de production.
- 7 Mettez hors tension l'environnement de migration de test une fois la migration de production terminée. L'exécution des deux systèmes vRealize Automation à long terme n'est pas une configuration prise en charge.

Interfaces utilisateur de l'environnement vRealize Automation

Utilisez et gérez votre environnement vRealize Automation avec plusieurs interfaces.

interfaces utilisateur

Ces tableaux décrivent les interfaces qui permettent de gérer votre environnement vRealize Automation.

Tableau 1-75. Console d'administration vRealize Automation

Objectif	Accès	Informations d'identification requises
Utilisez la console vRealize Automation pour ces tâches de l'administrateur système.	1 Démarrez un navigateur et ouvrez la page de démarrage du dispositif vRealize Automation en utilisant le nom de domaine complet du dispositif virtuel :	Vous devez être un utilisateur disposant du rôle administrateur système.
■ Ajouter des locataires.		
■ Personnaliser l'interface utilisateur vRealize Automation.	https://vrealize-automation-appliance-FQDN .	
■ Configurer les serveurs de messagerie.	2 Cliquez sur vRealize Automation Console .	Vous pouvez également utiliser cette URL pour ouvrir la console vRealize Automation : https://vrealize-automation-appliance-FQDN/vcac
■ Afficher les journaux des événements.		
■ Configurez vRealize Orchestrator.		
	3 Connectez-vous.	

Tableau 1-76. Console de locataire vRealize Automation. Cette interface est l'interface utilisateur principale que vous utilisez pour créer et gérer vos services et ressources.

Objectif	Accès	Informations d'identification requises
Utilisez vRealize Automation pour ces tâches.	1 Démarrez un navigateur et entrez l'URL de votre locataire en utilisant le nom de domaine complet du dispositif virtuel et le nom de l'URL du locataire :	Vous devez être un utilisateur disposant d'un ou de plusieurs de ces rôles :
■ Demander de nouveaux Blueprints de service informatique.	https://vrealize-automation-appliance-FQDN/vcac/org/tenant_URL_name .	
■ Créer et gérer des ressources cloud et informatiques.	2 Connectez-vous.	<ul style="list-style-type: none"> ■ Architecte d'application ■ Administrateur d'approbations ■ Administrateur du catalogue ■ Administrateur de conteneur ■ Architecte de conteneur ■ Consommateur de santé ■ Architecte d'infrastructure ■ Consommateur d'exportation sécurisée ■ Architecte de logiciel ■ Administrateur de locataire ■ Architecte XaaS
■ Créer et gérer des groupes personnalisés.		
■ Créer et gérer des groupes d'activité.		
■ Attribuer des rôles aux utilisateurs		

Tableau 1-77. Interface de gestion du dispositif vRealize Automation.

Objectif	Accès	Informations d'identification requises
<p>Utilisez la gestion des dispositifs vRealize Automation pour ces tâches.</p> <ul style="list-style-type: none"> ■ Afficher l'état des services enregistrés. ■ Afficher les informations système et redémarrer ou arrêter le dispositif. ■ Gérer la participation au Programme d'amélioration du produit. ■ Afficher l'état du réseau. ■ Afficher l'état de mise à jour et installer les mises à jour. ■ Gérer les paramètres d'administration. ■ Gérer les paramètres de l'hôte vRealize Automation. ■ Gérer les paramètres SSO. ■ Gérer les licences des produits. ■ Configurer la base de données Postgres vRealize Automation. ■ Configurer la messagerie vRealize Automation. ■ Configurer la journalisation vRealize Automation. ■ Installer les composants IaaS. ■ Migrer à partir d'une installation vRealize Automation existante ■ Gérer les certificats des composants IaaS ■ Configurer le service Xenon. 	<ol style="list-style-type: none"> 1 Démarrez un navigateur et ouvrez la page de démarrage du dispositif vRealize Automation en utilisant le nom de domaine complet du dispositif virtuel : https://vrealize-automation-appliance-FQDN 2 Cliquez sur Gestion de dispositifs vRealize Automation. Vous pouvez également utiliser cette URL pour ouvrir l'interface de gestion du dispositif vRealize Automation : https://vrealize-automation-appliance-FQDN:5480 3 Connectez-vous. 	<ul style="list-style-type: none"> ■ Nom d'utilisateur : root ■ Mot de passe : mot de passe que vous avez entré lorsque vous avez déployé le dispositif vRealize Automation.

Tableau 1-78. Client vRealize Orchestrator

Objectif	Accès	Informations d'identification requises
<p>Utilisez le client vRealize Orchestrator pour effectuer ces tâches.</p> <ul style="list-style-type: none"> ■ Développer des actions. ■ Développer des workflows. ■ Gérer des stratégies. ■ Installer des modules. ■ Gérer les autorisations d'utilisateur et de groupe d'utilisateurs. ■ Attacher des balises à des objets URI. ■ Afficher l'inventaire. 	<ol style="list-style-type: none"> 1 Démarrez un navigateur et ouvrez la page de démarrage vRealize Automation en utilisant le nom de domaine complet du dispositif virtuel : https://vrealize-automation-appliance-FQDN 2 Pour télécharger le fichier client.jnlp sur votre ordinateur local, cliquez sur vRealize Orchestrator Client. 3 Cliquez avec le bouton droit de la souris sur le fichier client.jnlp et sélectionnez Lancer. 4 Dans la boîte de dialogue Voulez-vous continuer ?, cliquez sur Continuer. 5 Connectez-vous. 	<p>Vous devez être un utilisateur disposant du rôle d'administrateur système ou appartenir au groupe vcoadmins configuré dans les paramètres de fournisseur d'authentification du centre de contrôle vRealize Orchestrator.</p>

Tableau 1-79. Centre de contrôle vRealize Orchestrator

Objectif	Accès	Informations d'identification requises
<p>Utilisez le centre de contrôle vRealize Orchestrator pour modifier la configuration de l'instance par défaut de vRealize Orchestrator qui est intégrée dans vRealize Automation.</p>	<ol style="list-style-type: none"> 1 Démarrez un navigateur et ouvrez la page de démarrage du dispositif vRealize Automation en utilisant le nom de domaine complet du dispositif virtuel : https://vrealize-automation-appliance-FQDN 2 Cliquez sur Gestion de dispositifs vRealize Automation. Vous pouvez également utiliser cette URL pour ouvrir l'interface de gestion du dispositif vRealize Automation : https://vrealize-automation-appliance-FQDN:5480 3 Connectez-vous. 4 Cliquez sur vRA > Orchestrator. 5 Sélectionnez l'interface utilisateur d'Orchestrator. 6 Cliquez sur Démarrer. 7 Cliquez sur l'URL de l'interface utilisateur d'Orchestrator. 8 Connectez-vous. 	<p>Nom d'utilisateur</p> <ul style="list-style-type: none"> ■ Entrez root si l'authentification basée sur les rôles n'est pas configurée. ■ Entrez votre nom d'utilisateur vRealize Automation s'il est configuré pour l'authentification basée sur les rôles. <p>Mot de passe</p> <ul style="list-style-type: none"> ■ Entrez le mot de passe que vous avez entré lorsque vous avez déployé le dispositif vRealize Automation si l'authentification basée sur les rôles n'est pas configurée. ■ Entrez le mot de passe de votre nom d'utilisateur si ce dernier est configuré pour l'authentification basée sur les rôles.

Tableau 1-80. Invite de commande Linux

Objectif	Accès	Informations d'identification requises
<p>Utilisez l'invite de commande Linux sur un hôte, tels que l'hôte du dispositif vRealize Automation, pour ces tâches.</p> <ul style="list-style-type: none"> ■ Arrêter ou démarrer les services ■ Modifier les fichiers de configuration ■ Exécuter des commandes ■ Récupérer des données 	<ol style="list-style-type: none"> 1 Sur l'hôte du dispositif vRealize Automation, ouvrez une nouvelle invite de commande. Pour ouvrir l'invite de commande sur votre ordinateur local, vous pouvez démarrer une session sur l'hôte à l'aide d'une application telle que PuTTY. 2 Connectez-vous. 	<ul style="list-style-type: none"> ■ Nom d'utilisateur : root ■ Mot de passe : mot de passe que vous avez créé lorsque vous avez déployé le dispositif vRealize Automation.

Tableau 1-81. Invite de commande Windows

Objectif	Accès	Informations d'identification requises
<p>Vous pouvez utiliser une invite de commande Windows sur un hôte, tel que l'hôte IaaS, pour exécuter des scripts.</p>	<ol style="list-style-type: none"> 1 Sur l'hôte IaaS, connectez-vous à Windows. Pour vous connecter à partir de votre ordinateur local, vous pouvez démarrer une session de poste de travail distante. 2 Ouvrez l'invite de commande Windows. Pour ouvrir l'invite de commande, cliquez avec le bouton droit sur l'icône Démarrer sur l'hôte et sélectionnez Invite de commande ou Invite de commande (admin). 	<ul style="list-style-type: none"> ■ Nom d'utilisateur : utilisateur disposant de privilèges administratifs. ■ Mot de passe : mot de passe de l'utilisateur.

Conditions préalables à la migration

Les conditions préalables à la migration varient en fonction de votre environnement cible.

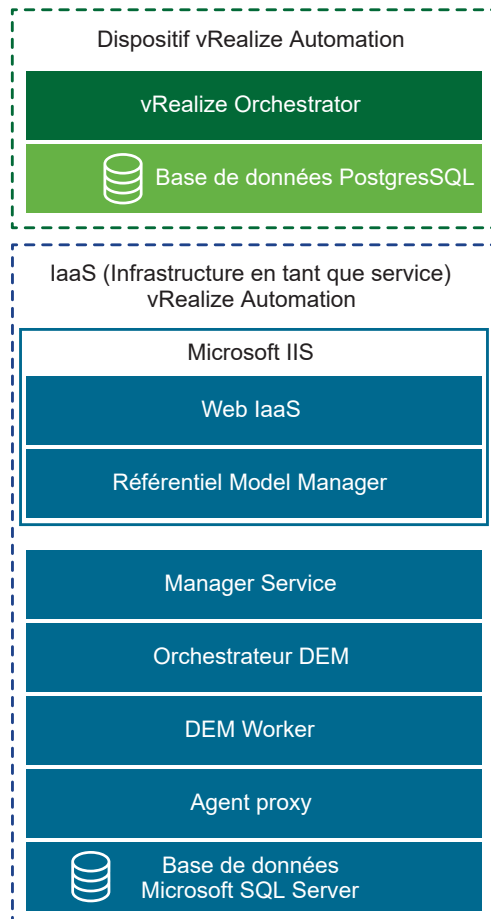
Vous pouvez migrer vers un environnement minimal ou vers un environnement à haute disponibilité.

Conditions préalables à la migration vers un environnement minimal

Assurez-vous une migration réussie dans un environnement minimal en consultant les conditions préalables suivantes.

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

Figure 1-16. Déploiement vRealize Automation minimal



Conditions préalables

- Vérifiez que vous disposez d'un nouvel environnement cible de vRealize Automation.
- Installez les agents proxy appropriés sur l'environnement cible en fonction de ces conditions requises.
 - Le nom de l'agent proxy cible doit correspondre au nom de l'agent proxy source pour les agents proxy vSphere, Hyper-V, Citrix XenServer et Test.

Note Terminez ces étapes pour obtenir un nom d'agent.

- 1 Sur l'hôte IaaS, connectez-vous à Windows en tant qu'utilisateur local avec des privilèges d'**administrateur**.
 - 2 Utilisez l'Explorateur Windows pour accéder au répertoire d'installation de l'agent.
 - 3 Ouvrez le fichier VRMAgent.exe.config.
 - 4 Sous la balise serviceConfiguration, recherchez la valeur de l'attribut agentName.
- Consultez l'article [51531](#) de la base de connaissances.

- Le nom du point de terminaison de l'agent proxy cible doit correspondre au nom du point de terminaison de l'agent proxy source pour les agents proxy vSphere, Hyper-V, Citrix XenServer et Test.
- Ne créez pas de point de terminaison pour les agents proxy vSphere, Hyper-V, Citrix XenServer ou Test sur l'environnement cible.
- Vérifiez les numéros de version des composants vRealize Automation sur le dispositif vRealize Automation cible.
 - a Connectez-vous à la gestion des dispositifs vRealize Automation cible en tant qu'**utilisateur racine** à l'aide du mot de passe que vous avez entré lorsque vous avez déployé le dispositif vRealize Automation cible.
 - b Sélectionnez **Cluster**.
 - c Développez les enregistrements de nom d'hôte/de nœud en cliquant sur le triangle. Vérifiez que les numéros de version des composants vRealize AutomationIaaS correspondent.
- Assurez-vous que la version cible de Microsoft SQL Server pour la base de données vRealize AutomationIaaS cible est 2012, 2014 ou 2016.
- Vérifiez que le port 22 est ouvert entre les environnements vRealize Automation source et cible. Le port 22 est requis pour établir des connexions SSH (Secure Shell) entre les dispositifs virtuels source et cible.
- Vérifiez que le point de terminaison vCenter dispose de ressources suffisantes pour effectuer la migration.
- Vérifiez que l'heure système de l'environnement vRealize Automation cible est synchronisée entre Cafe et les composants IaaS.
- Vérifiez que l'environnement d'exécution JRE (Java SE Runtime Environment) 8 (64 bits), Update 181 ou version ultérieure est installé au minimum pour chaque nœud de serveur IaaS de l'environnement cible. Après avoir installé JRE, vérifiez que la variable d'environnement JAVA_HOME pointe vers la version de Java que vous avez installée sur chaque nœud IaaS. Modifiez le chemin d'accès si nécessaire.
- Vérifiez que chaque nœud IaaS PowerShell 3.0 ou version ultérieure est installé.
- Assurez-vous que les environnements vRealize Automation source et cible sont en cours d'exécution.
- Vérifiez qu'aucune activité d'utilisateur ou de provisionnement n'est en cours sur l'environnement vRealize Automation source.
- Vérifiez que les logiciels antivirus ou de sécurité exécutés sur les nœuds IaaS dans l'environnement vRealize Automation pouvant interagir avec le système d'exploitation et ses composants cibles sont correctement configurés ou désactivés.

- Vérifiez que les dispositifs IaaS Web Service et Model Manager ne pas doivent être redémarrés en raison de mises à jour d'installation de Windows en attente. Les mises à jour en attente peuvent empêcher la migration de démarrer ou arrêter le Service de publication World Wide Web.

Étape suivante

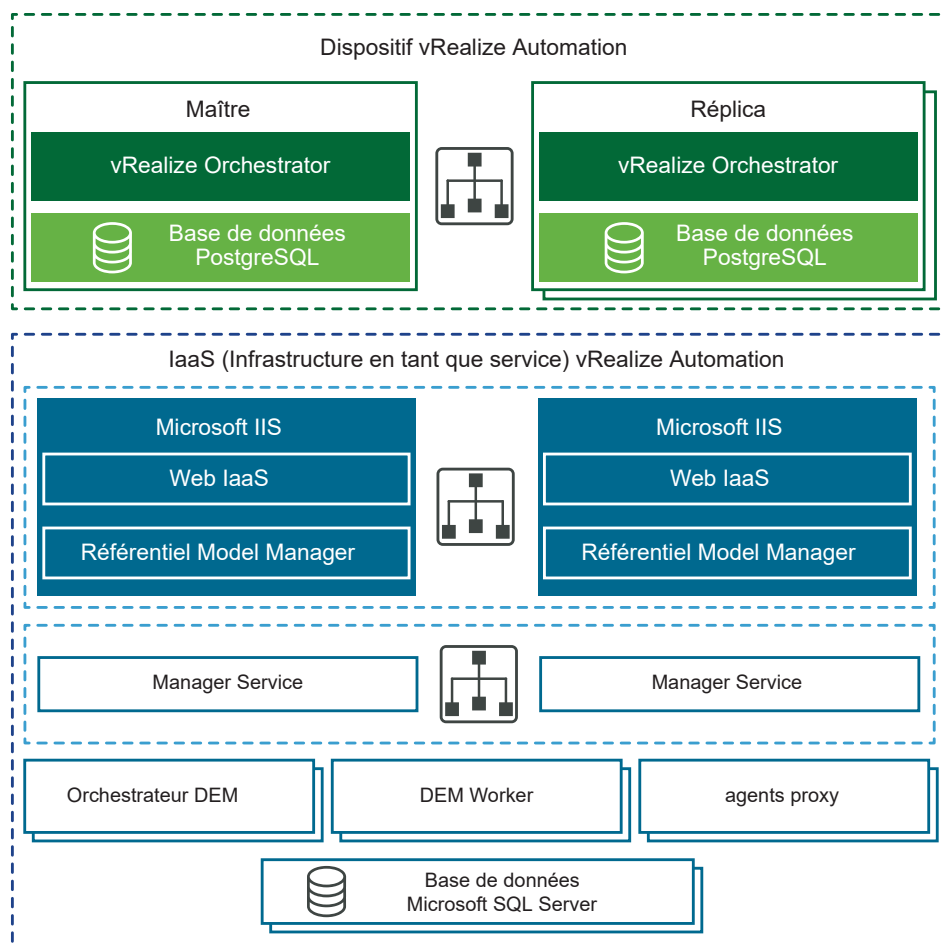
Tâches préalables à la migration.

Conditions préalables à la migration vers un environnement à haute disponibilité

Pour garantir une migration réussie vers un environnement de haute disponibilité, passez en revue ces conditions requises.

Les environnements à haute disponibilité peuvent être de différentes tailles. Un déploiement distribué de base peut améliorer vRealize Automation simplement en hébergeant des composants IaaS sur des serveurs Windows distincts. De nombreux environnements à haute disponibilité vont même plus loin, avec des dispositifs redondants, des serveurs redondants et un équilibrage de charge pour offrir une capacité supérieure. Les grands déploiements distribués offrent une meilleure échelle, une haute disponibilité et une récupération d'urgence.

Figure 1-17. Environnement vRealize Automation à haute disponibilité



Conditions préalables

- Assurez-vous que vous disposez d'une nouvelle installation cible de vRealize Automation avec un dispositif virtuel master et de réplica configuré pour la haute disponibilité. Reportez-vous à la section [Considérations relatives à la configuration de vRealize Automation haute disponibilité](#).
- Vérifiez que tous les dispositifs virtuels vRealize Automation utilisent le même mot de passe pour l'utilisateur racine.
- Installez les agents proxy appropriés sur l'environnement cible en fonction de ces conditions requises.
 - Le nom de l'agent proxy cible doit correspondre au nom de l'agent proxy source pour les agents proxy vSphere, Hyper-V, Citrix XenServer et Test.

Note Terminez ces étapes pour obtenir un nom d'agent.

- 1 Sur l'hôte IaaS, connectez-vous à Windows en tant qu'utilisateur local avec des privilèges d'**administrateur**.
 - 2 Utilisez l'Explorateur Windows pour accéder au répertoire d'installation de l'agent.
 - 3 Ouvrez le fichier `VRMAgent.exe.config`.
 - 4 Sous la balise `serviceConfiguration`, recherchez la valeur de l'attribut `agentName`.
-
- Le nom du point de terminaison de l'agent proxy cible doit correspondre au nom du point de terminaison de l'agent proxy source pour les agents proxy vSphere, Hyper-V, Citrix XenServer et Test.
 - Ne créez pas de point de terminaison pour les agents proxy vSphere, Hyper-V, Citrix XenServer ou Test sur l'environnement cible.
 - Vérifiez les numéros de version des composants vRealize Automation sur le dispositif vRealize Automation cible.
 - a Dans votre environnement vRealize Automation racine, connectez-vous à l'interface de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.
`https://vrealize-automation-appliance-FQDN:5480`
 - b Sélectionnez **Cluster**.
 - c Pour développer les enregistrements de nom d'hôte/de nœud afin d'afficher les composants, cliquez sur le bouton Développer.

Vérifiez que les numéros de version des composants vRealize Automation correspondent dans tous les nœuds de dispositif virtuel.

Vérifiez que les numéros de version des composants vRealize AutomationIaaS correspondent dans tous les nœuds IaaS.
 - Consultez l'article [51531](#) de la base de connaissances.

- Procédez comme suit pour diriger le trafic uniquement vers le nœud master.
 - a Désactivez tous les nœuds redondants.
 - b Supprimez les moniteurs de santé pour ces éléments conformément à la documentation de votre équilibrage de charge :
 - Dispositif virtuel vRealize Automation
 - Site Web IaaS
 - IaaS Manager Service
- Assurez-vous que la version cible de Microsoft SQL Server pour la base de données vRealize Automation IaaS cible est 2012, 2014 ou 2016.
- Vérifiez que le port 22 est ouvert entre les environnements vRealize Automation source et cible. Le port 22 est requis pour établir des connexions SSH (Secure Shell) entre les dispositifs virtuels source et cible.
- Vérifiez que le point de terminaison vCenter dispose de ressources suffisantes pour effectuer la migration.
- Assurez-vous d'avoir modifié les paramètres du délai d'expiration d'équilibrage de charge de la valeur par défaut à au moins 10 minutes.
- Vérifiez que l'heure système de l'environnement vRealize Automation cible est synchronisée entre Cafe et les composants IaaS.
- Vérifiez que les nœuds IaaS Web Service et Model Manager dans l'environnement cible disposent de l'environnement d'exécution Java approprié. L'environnement d'exécution Java SE (JRE) 8, 64 bits, Update 181 ou version ultérieure doit être installé. Assurez-vous que la variable système JAVA_HOME pointe vers la version de Java que vous avez installée sur chaque nœud IaaS. Modifiez le chemin d'accès si nécessaire.
- Vérifiez que chaque nœud IaaS dispose au minimum de PowerShell 3.0 ou version ultérieure.
- Assurez-vous que les environnements vRealize Automation source et cible sont en cours d'exécution.
- Vérifiez qu'aucune activité d'utilisateur ou de provisionnement n'est en cours sur l'environnement vRealize Automation source.
- Vérifiez que les logiciels antivirus ou de sécurité exécutés sur les nœuds IaaS dans l'environnement vRealize Automation pouvant interagir avec le système d'exploitation et ses composants cibles sont correctement configurés ou désactivés.
- Vérifiez que les dispositifs IaaS Web Service et Model Manager ne pas doivent être redémarrés en raison de mises à jour d'installation de Windows en attente. Les mises à jour en attente peuvent empêcher la migration de démarrer ou arrêter le Service de publication World Wide Web.

Étape suivante

Tâches préalables à la migration.

Tâches préalables à la migration

Avant de migrer, vous devez effectuer plusieurs tâches préalables à la migration.

Les tâches préalables à la migration que vous effectuez avant de migrer les données de votre environnement vRealize Automation source vers l'environnement vRealize Automation cible varient en fonction de votre environnement source.

Passer en revue les modifications introduites par la migration de vRealize Automation

vRealize Automation 7.1 et versions ultérieures introduit diverses modifications fonctionnelles pendant et après la mise à niveau. Si vous mettez à niveau à partir d'un environnement vRealize Automation 6.2.5, passez en revue ces modifications avant de commencer le processus de mise à niveau.

Pour plus d'informations sur les différences entre vRealize Automation 6.2.5, 7.1 et versions supérieures, reportez-vous à la section [Passer en revue les modifications introduites par la migration de vRealize Automation](#).

Note L'outil assistant de mise à jour de test de production vRealize analyse votre environnement vRealize Automation 6.2.5, recherche les configurations de fonctionnalités qui peuvent entraîner des problèmes de mise à niveau et vérifie que votre environnement est prêt pour la mise à niveau. Pour télécharger cet outil et la documentation associée, accédez à la page de téléchargement du produit [Outil de test de production VMware vRealize](#).

Après la migration de vRealize Automation 6.2.5 vers la dernière version, les éléments de catalogue qui utilisent ces définitions de propriétés s'affichent dans le catalogue de services, mais ne sont pas disponibles pour les demandes.

- Types de contrôle : case à cocher ou lien.
- Attributs : relation, expressions régulières ou dispositions de propriétés.

Dans vRealize Automation 7.1 et versions ultérieures, les définitions de propriétés n'utilisent plus ces éléments. Vous devez créer à nouveau la définition de propriété ou la configurer de façon à utiliser une action de script vRealize Orchestrator au lieu des types de contrôle ou d'attribut intégrés. Pour plus d'informations, reportez-vous à [Les éléments de catalogue figurent dans le catalogue de services après la migration mais ne sont pas disponibles pour les demandes](#).

Appliquer le correctif de l'agent logiciel

Avant de migrer vRealize Automation 7.1.x ou 7.3.x, vous devez appliquer un correctif au dispositif source afin de pouvoir mettre à niveau les agents logiciels vers TLS 1.2.

Le protocole TLS (Transport Layer Security) assure l'intégrité des données entre votre navigateur et vRealize Automation. Ce correctif permet aux agents logiciels de votre environnement source de procéder à une mise à niveau vers TLS 1.2. Cette mise à niveau attribue le niveau de sécurité le plus élevé et est requise pour vRealize Automation 7.1.x ou 7.3.x. Chaque version possède son propre correctif.

Conditions préalables

Un environnement vRealize Automation source 7.1.x ou 7.3.x vRealize Automation en cours d'exécution.

Procédure

- ◆ Appliquez ce correctif à votre dispositif 7.1.x ou 7.3.x vRealize Automation source avant de commencer la migration. Consultez [l'article 52897 de la base de connaissances](#).

Étape suivante

[Passer le paramètre DoDeletes de l'agent vSphere sur False.](#)

Passer le paramètre DoDeletes de l'agent vSphere sur False

Si vous migrez d'un environnement vRealize Automation 6.2.x, vous devez modifier la valeur DoDeletes de **true** à **false** sur votre agent vSphere cible avant la migration.

Conditions préalables

Terminez les conditions préalables pour la migration.

Procédure

- 1 Passez la valeur DoDeletes en **false**.

Cela empêche de supprimer vos machines virtuelles de l'environnement source. Les environnements source et cible s'exécutent en parallèle. Des décalages de bail peuvent se produire après que la migration de production est validée.

- 2 Définissez la valeur DoDeletes sur **true** après que la migration de votre production est validée et que votre environnement source est arrêté.
- 3 Suivez les étapes de la procédure [Configurer l'agent vSphere](#) pour définir DoDeletes sur **false**.

Étape suivante

[Préparer les machines virtuelle vRealize Automation pour la migration.](#)

Vérifier les modèles dans votre environnement vRealize Automation source

Avant de migrer vRealize Automation, vous devez vérifier vos modèles de machine virtuelle pour vous assurer que chaque modèle dispose d'un paramètre de mémoire minimale d'au moins 4 Mo.

Si vous disposez d'un modèle de machine virtuelle dans votre environnement vRealize Automation source avec moins de 4 Mo de mémoire, la migration échoue. Effectuez cette procédure pour déterminer si des Blueprints dans l'environnement source disposent de moins de 4 Mo de mémoire.

Conditions préalables

Procédure

- 1 Connectez-vous au serveur Windows hébergeant votre base de données SQL Server.
- 2 Ouvrez SQL Server Management Studio et connectez-vous à votre base de données vRA.
- 3 Exécutez ce script pour vérifier si des Blueprints disposent d'une mémoire spécifiée inférieure à 4 Mo.

```
select VirtualMachineTemplate set MemoryMB = 4 where IsHidden = 0 and MemoryMB < 4;
```

où vCAC est le nom de la base de données.

- 4 Si le script détecte des Blueprints disposant d'une mémoire spécifiée inférieure à 4 Mo, exécutez ce script pour mettre à jour la mémoire à au moins 4 Mo.

```
update [vCAC].[dbo].[VirtualMachineTemplate] set MemoryMB = 4 where IsHidden = 0 and MemoryMB < 4;
```

où vCAC est le nom de la base de données.

Étape suivante

[Préparer les machines virtuelle vRealize Automation pour la migration.](#)

Préparer les machines virtuelle vRealize Automation pour la migration

Les problèmes connus liés à la migration des machines virtuelles 6.2.x vRealize Automation peuvent causer des problèmes après la migration.

Vous devez vérifier [l'article 000051531 de la base de connaissances](#) et effectuer tous les correctifs appropriés à vos environnements avant la migration.

Étape suivante

[Collecter les informations requises pour la migration.](#)

Collecter les informations requises pour la migration

Utilisez ces tables pour enregistrer les informations dont vous avez besoin pour la migration à partir de vos environnements source et cible.

Conditions préalables

Terminez la vérification des conditions préalables s'appliquant à votre situation.

- [Conditions préalables à la migration vers un environnement minimal.](#)
- [Conditions préalables à la migration vers un environnement à haute disponibilité.](#)

Exemple

Tableau 1-82. Dispositif vRealize Automation source

Option	Description	Valeur
Nom d'hôte	Connectez-vous à votre gestion de dispositifs vRealize Automation source. Recherchez le nom d'hôte dans l'onglet Système . Le nom d'hôte doit être un nom de domaine complet.	
Nom d'utilisateur racine	root	
Mot de passe racine	Mot de passe de l'utilisateur racine que vous avez entré lorsque vous avez déployé votre dispositif vRealize Automation source.	
Emplacement du module de migration	Chemin d'accès à un répertoire existant sur le dispositif vRealize Automation 6.2.x ou 7.x source sur lequel le module de migration est créé. Le répertoire doit contenir un espace disponible équivalent à deux fois la taille de la base de données vRealize Automation. L'emplacement par défaut est /storage.	

Tableau 1-83. Dispositif vRealize Automation cible

Option	Description	Valeur
Nom d'utilisateur racine	root	
Mot de passe racine	Mot de passe de l'utilisateur racine que vous avez entré lorsque vous avez déployé votre vRealize Automation cible.	
Locataire par défaut	vsphere.local	
Nom d'utilisateur de l'administrateur	administrateur	
Mot de passe de l'administrateur	Mot de passe de l'utilisateur administrator@vsphere.local que vous avez entré lors du déploiement de l'environnement vRealize Automation cible.	

Tableau 1-84. Base de données IaaS cible

Option	Description	Valeur
Serveur de base de données	Emplacement de l'instance de Microsoft SQL Server sur lequel réside la base de données clonée. Si une instance nommée et un port autre que le port par défaut sont utilisés, spécifiez l'option au format SERVEUR,PORT\NOM-INSTANCE.	
Nom de la base de données clonée	Nom de la base de données vRealize Automation 6.2.x/7.x IaaS Microsoft SQL source clonée pour la migration.	

Tableau 1-84. Base de données IaaS cible (suite)

Option	Description	Valeur
Mode d'authentification	Sélectionnez Windows ou SQL Server. Si vous sélectionnez l'option SQL Server, vous devez entrer un nom de connexion et un mot de passe.	
Nom de connexion	Nom de connexion de l'utilisateur SQL Server disposant du rôle db_owner pour la base de données Microsoft SQL IaaS clonée.	
Mot de passe	Mot de passe de l'utilisateur SQL Server.	
Clé de chiffrement d'origine	Clé de chiffrement d'origine que vous récupérez depuis l'environnement source. Reportez-vous à Obtenir la clé de chiffrement à partir de l'environnement vRealize Automation source .	
Nouvelle phrase secrète	Série de mots utilisés pour générer une nouvelle clé de chiffrement. Vous utilisez cette phrase secrète chaque fois que vous installez un nouveau composant IaaS dans l'environnement vRealize Automation cible.	

Étape suivante

[Obtenir la clé de chiffrement à partir de l'environnement vRealize Automation source.](#)

Obtenir la clé de chiffrement à partir de l'environnement vRealize Automation source

Vous devez entrer la clé de chiffrement depuis l'environnement vRealize Automation source dans le cadre de la procédure de migration.

Conditions préalables

Vérifiez que vous disposez des privilèges d'administrateur sur la machine virtuelle de l'hôte Manager Service active dans votre environnement source.

Procédure

- 1 Ouvrez une invite de commandes en tant qu'administrateur de la machine virtuelle qui héberge le composant Manager Service actif dans votre environnement source et exécutez la commande suivante.

```
"C:\Program Files (x86)\VMware\VCAC\Server\ConfigTool\EncryptionKeyTool\DynamicOps.Tools.EncryptionKeyTool.exe" key-read -c "C:\Program Files (x86)\VMware\VCAC\Server\ManagerService.exe.config" -v
```

Si votre répertoire d'installation ne se situe pas à l'emplacement par défaut, à savoir C:\Program Files (x86)\VMware\VCAC, modifiez le chemin pour qu'il reflète celui de votre répertoire d'installation réel.

- 2 Enregistrez la clé qui s'affiche après l'exécution de la commande.

La clé est une longue chaîne de caractères ayant un aspect similaire à l'exemple suivant :

NRH+f/B1nCB6yvasLS3sxespgdkcFWAEuyV0g41fryg=.

Étape suivante

- Si vous effectuez une migration à partir d'un environnement vRealize Automation 6.2.x : [Ajouter chaque locataire à l'environnement cible à partir de l'environnement source de vRealize Automation.](#)
- Si vous effectuez une migration à partir d'un environnement vRealize Automation 7.x : [Répertorier les administrateurs de locataires et les administrateurs IaaS depuis l'environnement vRealize Automation 6.2.x source.](#)

Répertorier les administrateurs de locataires et les administrateurs IaaS depuis l'environnement vRealize Automation 6.2.x source

Avant de migrer un environnement vRealize Automation 6.2.x, vous devez créer la liste des administrateurs de locataires et des administrateurs IaaS pour chaque locataire.

Procédez comme suit pour chaque locataire dans la console vRealize Automation source.

Note Si vous effectuez la migration depuis un environnement vRealize Automation 7.x, vous pouvez ignorer cette procédure.

Conditions préalables

Connectez-vous à la console vRealize Automation source en tant qu'**administrateur** avec le mot de passe que vous avez entré lorsque vous avez déployé le dispositif source vRealize Automation.

Note Pour un environnement à haute disponibilité, ouvrez la console en utilisant le nom de domaine complet de l'équilibrage de charge du dispositif virtuel source : `https://vra-va-lb-hostname.Domain.Name/vcac`.

Procédure

- 1 Sélectionnez **Administration > Locataires**.
- 2 Cliquez sur le nom d'un locataire.
- 3 Cliquez sur **Administrateurs**.
- 4 Répertoriez les noms d'utilisateur de chaque administrateur de locataires et de chaque administrateur IaaS.
- 5 Cliquez sur **Annuler**.

Étape suivante

[Ajouter chaque locataire à l'environnement cible à partir de l'environnement source de vRealize Automation.](#)

Ajouter chaque locataire à l'environnement cible à partir de l'environnement source de vRealize Automation

Vous devez ajouter des locataires dans l'environnement cible à l'aide du nom de chaque locataire dans l'environnement source.

Pour une migration réussie, il est obligatoire que chaque locataire de l'environnement source soit créé dans l'environnement cible. Vous devez également utiliser une URL d'accès spécifique à un locataire pour chaque locataire que vous ajoutez à l'aide du nom d'URL de locataire de l'environnement source. S'il existe des locataires inutilisés dans l'environnement source que vous ne voulez pas migrer, supprimez-les de l'environnement source avant la migration.

Note La validation de la migration garantit que le système cible possède au moins les mêmes locataires configurés dans la source que ceux requis par les conditions préalables. Il effectue la comparaison des locataires sur la base des noms d'URL des locataires sensibles à la casse, et non sur la base des noms des locataires.

Effectuez cette procédure pour chaque locataire de votre environnement source.

- Lorsque vous effectuez une migration à partir d'un environnement vRealize Automation 6.2.x, vous migrez vos locataires SSO2 et magasins d'identités existants de l'environnement source vers le VMware Identity Manager dans l'environnement cible.
- Lorsque vous effectuez une migration à partir d'un environnement vRealize Automation 7.x, vous migrez vos locataires VMware Identity Manager et magasins d'identités existants de l'environnement source vers le VMware Identity Manager dans l'environnement cible.

Conditions préalables

- [Collecter les informations requises pour la migration.](#)
- Connectez-vous à la console vRealize Automation cible en tant qu'**administrateur** avec le mot de passe que vous avez entré lorsque vous avez déployé le dispositif vRealize Automation cible.

Note Pour un environnement à haute disponibilité, ouvrez la console à l'aide du nom de domaine complet de l'équilibrage de charge du dispositif virtuel cible : `https://vra-va-lb-hostname.domain.name/vcac`.

Procédure

- 1 Sélectionnez **Administration > Locataires**.
- 2 Cliquez sur l'icône **Nouveau** (+).
- 3 Dans la zone de texte **Nom**, entrez un nom de locataire qui correspond à un nom de locataire dans l'environnement source.

Par exemple, si le nom du locataire de l'environnement source est DEVTenant, entrez **DEVTenant**.
- 4 (Facultatif) Entrez une description dans la zone de texte **Description**.

- 5 Dans la zone de texte **Nom de l'URL**, entrez un nom d'URL de locataire correspondant au nom de l'URL du locataire de l'environnement source.

Ce nom d'URL est utilisé pour ajouter un identifiant spécifique au locataire à l'URL de la console vRealize Automation.

Par exemple, si le nom de l'URL de DEVTenant dans l'environnement source est dev, entrez **dev** pour créer l'URL `https://vra-vb-hostname.domain.name/vcac/org/dev`.

- 6 (Facultatif) Entrez une adresse e-mail dans la zone de texte **e-mail de contact**.
- 7 Cliquez sur **Envoyer et Suivant**.

Étape suivante

[Créer un administrateur pour chaque locataire ajouté.](#)

Créer un administrateur pour chaque locataire ajouté

Vous devez créer un administrateur pour chaque locataire ajouté à l'environnement cible. Créez un administrateur en créant un compte d'utilisateur local et en attribuant des privilèges d'administrateur de locataire au compte d'utilisateur local.

Effectuez cette procédure pour chaque locataire dans votre environnement cible.

Conditions préalables

- [Ajouter chaque locataire à l'environnement cible à partir de l'environnement source de vRealize Automation.](#)
- Connectez-vous à la console vRealize Automation cible en tant qu'**administrateur** avec le mot de passe que vous avez entré lorsque vous avez déployé le dispositif vRealize Automation cible.

Note Pour un environnement à haute disponibilité, ouvrez la console à l'aide du nom de domaine complet de l'équilibrage de charge du dispositif virtuel cible : `https://vra-vb-lb-hostname.domain.name/vcac`.

Procédure

- 1 Sélectionnez **Administration > Locataires**.
- 2 Cliquez sur un locataire que vous avez ajouté.
Par exemple, pour DEVTenant, cliquez sur **DEVTenant**.
- 3 Cliquez sur **Utilisateurs locaux**.
- 4 Cliquez sur l'icône **Nouveau** (+).
- 5 Dans **Détails de l'utilisateur**, entrez les informations demandées pour créer un compte d'utilisateur local afin d'attribuer le rôle d'administrateur de locataire.
Le nom d'utilisateur local doit être unique dans l'annuaire local par défaut, vsphere.local.

- 6 Cliquez sur **OK**.
- 7 Cliquez sur **Administrateurs**.
- 8 Entrez le nom d'utilisateur local dans la zone de recherche **Administrateurs de locataire** et appuyez sur Entrée.
- 9 Cliquez sur le nom approprié dans les résultats de recherche pour ajouter l'utilisateur à la liste des administrateurs de locataire.
- 10 Cliquez sur **Terminer**.
- 11 Déconnectez-vous de la console.

Étape suivante

- Pour un déploiement minimal : [Synchroniser les utilisateurs et les groupes pour un lien Active Directory avant la migration vers un environnement minimal](#).
- Pour un déploiement haute disponibilité : [Synchroniser les utilisateurs et les groupes pour un lien Active Directory avant la migration vers un environnement à haute disponibilité](#).

Synchroniser les utilisateurs et les groupes pour un lien Active Directory avant la migration vers un environnement minimal

Avant d'importer vos utilisateurs et vos groupes dans un déploiement minimal de vRealize Automation, vous devez connecter l'instance de vRealize Automation cible à votre lien Active Directory.

Effectuez cette procédure pour chaque locataire. Si un locataire dispose de plusieurs annuaires Active Directory, effectuez cette procédure pour chaque annuaire Active Directory utilisé par le locataire.

Conditions préalables

- [Créer un administrateur pour chaque locataire ajouté](#).
- Vérifiez que vous disposez de privilèges d'accès à l'annuaire Active Directory.
- Connectez-vous à vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

- 1 Sélectionnez **Administration > Gestion des annuaires > Annuaires**.
- 2 Cliquez sur l'icône **Ajouter un annuaire** (+) et sélectionnez **Ajouter Active Directory via LDAP/IWA**.

3 Entrez les paramètres de compte Active Directory.

◆ Pour les annuaires Active Directory non natifs

Option	Exemple d'entrée
Nom de l'annuaire	Saisissez un nom d'annuaire unique. Sélectionnez Active Directory via LDAP lorsque vous utilisez un annuaire Active Directory non natif.
Ce répertoire prend en charge l'emplacement du service DNS	Désélectionnez cette option.
Nom unique de base	Entrez le nom unique (DN) du point de départ des recherches sur le serveur d'annuaire. Par exemple, cn=users,dc=rainpole,dc=local .
Nom unique de liaison	Entrez le nom unique (DN) complet, incluant le nom commun (CN), d'un compte d'utilisateur Active Directory qui dispose de privilèges de recherche d'utilisateurs. Par exemple, cn=config_admin infra,cn=users,dc=rainpole,dc=local .
Mot de passe du nom unique de liaison	Entrez le mot de passe Active Directory du compte pouvant rechercher des utilisateurs et cliquez sur Tester la connexion pour tester la connexion au répertoire configuré.

◆ Pour les annuaires Active Directory natifs

Option	Exemple d'entrée
Nom de l'annuaire	Saisissez un nom d'annuaire unique. Sélectionnez Active Directory (authentification Windows intégrée) lorsque vous utilisez un répertoire Active Directory natif.
Nom de domaine	Entrez le nom du domaine à joindre.
Nom d'utilisateur de l'administrateur du domaine	Entrez le nom d'utilisateur de l'administrateur de domaine.
Mot de passe de l'administrateur du domaine	Entrez le mot de passe de l'administrateur du domaine.
UPN de l'utilisateur Bind	Utilisez le format d'adresse électronique pour entrer le nom de l'utilisateur pouvant s'authentifier auprès du domaine.
Mot de passe du nom unique de liaison	Entrez le mot de passe Bind Active Directory du compte autorisé à rechercher des utilisateurs.

4 Cliquez sur **Enregistrer et Suivant**.

Sélectionner les domaines affiche une liste de domaines.

5 Acceptez le paramètre du domaine par défaut et cliquez sur **Suivant**.

6 Vérifiez que les noms d'attribut sont mappés sur les bons attributs d'Active Directory et cliquez sur **Suivant**.

7 Sélectionnez les groupes et les utilisateurs à synchroniser.

- a Cliquez sur l'icône **Nouveau** (+).
- b Entrez le domaine de l'utilisateur et cliquez sur **Rechercher des groupes**.
Par exemple, entrez **dc=vcac,dc=local**.
- c Pour sélectionner les groupes à synchroniser, cliquez sur **Sélectionner**, puis sur **Suivant**.
- d Sur la page **Sélectionner des utilisateurs**, sélectionnez les utilisateurs que vous souhaitez synchroniser et cliquez sur **Suivant**.

Ajoutez uniquement des utilisateurs et des groupes requis pour l'utilisation de vRealize Automation. Ne sélectionnez pas l'option **Synchroniser les groupes imbriqués**, sauf si tous les groupes imbriqués sont requis pour l'utilisation de vRealize Automation.

8 Vérifiez les utilisateurs et les groupes que vous synchronisez avec l'annuaire et cliquez sur **Synchroniser l'annuaire**.

La synchronisation avec l'annuaire prend un certain temps et s'exécute en arrière-plan.

Étape suivante

[Exécuter la collecte de données réseau et de sécurité NSX dans l'environnement vRealize Automation source](#)

Synchroniser les utilisateurs et les groupes pour un lien Active Directory avant la migration vers un environnement à haute disponibilité

Avant d'importer vos utilisateurs et vos groupes dans un environnement vRealize Automation à haute disponibilité, vous devez vous connecter à votre lien Active Directory.

- Effectuez les étapes 1 à 8 pour chaque locataire. Si un locataire dispose de plusieurs annuaires Active Directory, effectuez cette procédure pour chaque annuaire Active Directory utilisé par le locataire.
- Répétez les étapes 9 à 10 pour chaque fournisseur d'identité associé à un locataire.

Conditions préalables

- [Créer un administrateur pour chaque locataire ajouté](#).
- Vérifiez que vous disposez de privilèges d'accès à l'annuaire Active Directory.
- Connectez-vous à vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

- 1 Sélectionnez **Administration > Gestion des annuaires > Annuaires**.
- 2 Cliquez sur l'icône **Ajouter un annuaire** (+) et sélectionnez **Ajouter Active Directory via LDAP/IWA**.

3 Entrez les paramètres de compte Active Directory.

◆ Pour les annuaires Active Directory non natifs

Option	Exemple d'entrée
Nom de l'annuaire	Saisissez un nom d'annuaire unique. Sélectionnez Active Directory via LDAP lorsque vous utilisez un annuaire Active Directory non natif.
Ce répertoire prend en charge l'emplacement du service DNS	Désélectionnez cette option.
Nom unique de base	Entrez le nom unique (DN) du point de départ des recherches sur le serveur d'annuaire. Par exemple, cn=users,dc=rainpole,dc=local .
Nom unique de liaison	Entrez le nom unique (DN) complet, incluant le nom commun (CN), d'un compte d'utilisateur Active Directory qui dispose de privilèges de recherche d'utilisateurs. Par exemple, cn=config_admin infra,cn=users,dc=rainpole,dc=local .
Mot de passe du nom unique de liaison	Entrez le mot de passe Active Directory du compte pouvant rechercher des utilisateurs et cliquez sur Tester la connexion pour tester la connexion au répertoire configuré.

◆ Pour les annuaires Active Directory natifs

Option	Exemple d'entrée
Nom de l'annuaire	Saisissez un nom d'annuaire unique. Sélectionnez Active Directory (authentification Windows intégrée) lorsque vous utilisez un répertoire Active Directory natif.
Nom de domaine	Entrez le nom du domaine à joindre.
Nom d'utilisateur de l'administrateur du domaine	Entrez le nom d'utilisateur de l'administrateur de domaine.
Mot de passe de l'administrateur du domaine	Entrez le mot de passe du compte de l'administrateur du domaine.
UPN de l'utilisateur Bind	Utilisez le format d'adresse électronique pour entrer le nom de l'utilisateur pouvant s'authentifier auprès du domaine.
Mot de passe du nom unique de liaison	Entrez le mot de passe Bind Active Directory du compte autorisé à rechercher des utilisateurs.


4 Cliquez sur **Enregistrer et Suivant**.

La page **Sélectionner les domaines** affiche la liste de domaines.

5 Acceptez le paramètre du domaine par défaut et cliquez sur **Suivant**.

6 Vérifiez que les noms d'attribut sont mappés sur les bons attributs d'Active Directory et cliquez sur **Suivant**.

7 Sélectionnez les groupes et les utilisateurs à synchroniser.

- a Cliquez sur l'icône **Nouveau** .
- b Entrez le domaine de l'utilisateur et cliquez sur **Rechercher des groupes**.
Par exemple, entrez **dc=vcac,dc=local**.
- c Pour sélectionner les groupes à synchroniser, cliquez sur **Sélectionner**, puis sur **Suivant**.
- d Sur la page **Sélectionner des utilisateurs**, sélectionnez les utilisateurs que vous souhaitez synchroniser et cliquez sur **Suivant**.

Ajoutez uniquement des utilisateurs et des groupes requis pour l'utilisation de vRealize Automation. Ne sélectionnez pas l'option **Synchroniser les groupes imbriqués**, sauf si tous les groupes imbriqués sont requis pour l'utilisation de vRealize Automation.

8 Vérifiez les utilisateurs et les groupes que vous synchronisez avec l'annuaire et cliquez sur **Synchroniser l'annuaire**.

La synchronisation avec l'annuaire prend un certain temps et s'exécute en arrière-plan.

9 Sélectionnez **Administration > Gestion des annuaires > Fournisseurs d'identité**, puis cliquez sur le nouveau fournisseur d'identité.

Par exemple, **WorkspaceIDP__1**.

10 Sur la page du fournisseur d'identité que vous avez sélectionné, ajoutez un connecteur pour chaque nœud.

- a Suivez les instructions pour **Ajouter un connecteur**.
- b Mettez à jour la valeur de la propriété **Nom d'hôte IdP** afin qu'elle pointe vers le nom de domaine complet (FQDN) de l'équilibrage de charge de vRealize Automation.
- c Cliquez sur **Enregistrer**.

Étape suivante

[Exécuter la collecte de données réseau et de sécurité NSX dans l'environnement vRealize Automation source.](#)

Exécuter la collecte de données réseau et de sécurité NSX dans l'environnement vRealize Automation source

Avant de migrer, vous devez exécuter la collecte de données d'inventaire réseau et de sécurité NSX dans l'environnement vRealize Automation source.

La collecte de données est nécessaire pour que l'action Reconfigurer l'équilibrage de charge fonctionne dans vRealize Automation après la migration à partir des versions 7.1.x ou ultérieures.

Note Vous n'avez pas besoin d'exécuter la collecte de données dans votre environnement source lorsque vous migrez depuis vRealize Automation 6.2.x. vRealize Automation 6.2.x ne prend pas en charge l'action Reconfiguration de l'équilibrage de charge.

Procédure

- ◆ Exécutez la collecte de données d'inventaire réseau et de sécurité NSX dans votre environnement vRealize Automation source avant de migrer vRealize Automation. Reportez-vous à la section [Démarrer la collecte de données de point de terminaison manuellement](#).

Étape suivante

[Cloner manuellement la base de données Microsoft SQL vRealize AutomationlaaS source.](#)

Cloner manuellement la base de données Microsoft SQL vRealize AutomationlaaS source

Avant la migration, vous devez sauvegarder votre base de données Microsoft SQL laaS dans l'environnement source vRealize Automation et la restaurer dans une nouvelle base de données vide créée dans l'environnement cible vRealize Automation.

Conditions préalables

- [Exécuter la collecte de données réseau et de sécurité NSX dans l'environnement vRealize Automation source.](#)
- Obtenez des informations sur la sauvegarde et la restauration d'une base de données SQL Server. Pour plus d'informations, recherchez des articles sur le [réseau de développeurs Microsoft](#) concernant la création d'une sauvegarde complète de base de données SQL Server et la restauration d'une base de données SQL Server à un nouvel emplacement.

Procédure

- ◆ Créez une sauvegarde complète de votre base de données Microsoft SQL vRealize AutomationlaaS source. Utilisez la sauvegarde pour restaurer la base de données SQL dans une nouvelle base de données vide créée dans l'environnement cible.

Étape suivante

[Snapshot de l'environnement vRealize Automation cible.](#)

Snapshot de l'environnement vRealize Automation cible

Prenez un snapshot de chaque machine virtuelle vRealize Automation cible. Si la migration échoue, vous pouvez essayer à nouveau en utilisant des snapshots de machines virtuelles.

Pour plus d'informations, reportez-vous à la documentation de vSphere.

Conditions préalables

[Cloner manuellement la base de données Microsoft SQL vRealize AutomationlaaS source.](#)

Étape suivante

Effectuez l'une des procédures suivantes :

- [Migrer les données sources vRealize Automation vers un environnement vRealize Automation minimal.](#)

- [Migrer les données source vRealize Automation vers un environnement vRealize Automation à haute disponibilité.](#)

Nettoyage de la base de données Postgres

Pour préparer votre base de données postgres pour la mise à niveau ou la migration, effectuez un nettoyage de la base de données.

Les objets volumineux du tableau pg_largeobject, qui stockent les bundles de journaux et de télémétrie, ainsi que les objets d'application, peuvent ralentir ou arrêter votre mise à niveau ou votre migration. Avant de tenter de mettre à niveau ou de migrer, vous pouvez préparer votre base de données postgres en effectuant un nettoyage de base de données à vide.

Note Le nettoyage de la base de données ne peut pas être effectué lorsque des services sont en cours d'exécution.

Procédure

- 1 Commencez par sauvegarder votre dispositif en créant un vidage de base de données postgres à partir de la page Cluster dans l'interface VAMI ou en effectuant ou sauvegardant un snapshot du dispositif virtuel master.
- 2 À partir de l'interface VAMI vRA, basculez la réplication de synchrone vers asynchrone.
- 3 En tant qu'utilisateur postgres sur le vRA master (su - postgres), videz la base de données pour supprimer les entrées du journal.

```
su - postgres -c "/opt/vmware/vpostgres/current/bin/vacuumlo -v -p 5432 vcac"
```

```
su - postgres -c "/opt/vmware/vpostgres/current/bin/vacuumdb -f -p 5432 -t pg_largeobject -t pg_largeobject_metadata vcac"
```

- 4 Pour récupérer de l'espace de base de données, utilisez les commandes de vidage complet.

```
psql -d vcac
vacuum full
vacuum analyze
```

Nettoyer les objets avec des noms de locataire en double

Avant de migrer vers vRealize Automation 7.x, vous devez nettoyer les objets avec des noms de locataire en double.

Pour nettoyer les objets avec des noms de locataire en double, suivez les étapes décrites dans l'article [KB 58002](#).

Nettoyer les ressources et les entrées de base de données vRealize Orchestrator en double

Avant de migrer vers vRealize Automation 7.x, vous devez nettoyer les ressources et les entrées de base de données vRealize Orchestrator en double.

Pour nettoyer les ressources et les entrées de base de données vRealize Orchestrator en double, suivez les étapes décrites dans l'article [KB 54987](#).

Sauvegarder les tables HF sur l'environnement vRealize Automation cible

Avant d'effectuer la migration vers vRealize Automation 7.x, vous devez sauvegarder les tables HF sur votre environnement vRealize Automation cible.

Si vous avez appliqué un correctif HF à votre environnement vRealize Automation 7.x, vous devez sauvegarder les tables HF avant la migration et les restaurer après la migration.

Pour sauvegarder les tables HF :

```
mkdir /tmp/hf_tables
/opt/vmware/vpostgres/current/bin/pg_dump -U postgres --data-only -d vcac -t public.hf_patch > /tmp/hf_tables/hf_patch.sql
/opt/vmware/vpostgres/current/bin/pg_dump -U postgres --data-only -d vcac -t public.hf_patch_execution > /tmp/hf_tables/hf_patch_execution.sql
/opt/vmware/vpostgres/current/bin/pg_dump -U postgres --data-only -d vcac -t public.hf_patch_nodes > /tmp/hf_tables/hf_patch_nodes.sql
cd /tmp/hf_tables/
zip -r /tmp/hf_tables.zip ./
```

Sauvegardez le fichier hf_tables.zip récemment créé.

Pour plus d'informations sur la restauration des tables HF après la migration, reportez-vous à la section [Restaurer les tables HF sur l'environnement vRealize Automation cible](#).

Procédures de migration

La procédure que vous effectuez pour migrer vos données d'environnement vRealize Automation source varie selon que vous migrez vers un environnement minimal ou vers un environnement haute disponibilité.

Migrer les données sources vRealize Automation vers un environnement vRealize Automation minimal

Vous pouvez migrer les données de votre environnement vRealize Automation actuel vers une nouvelle version de vRealize Automation.

Tous les locataires du système source doivent être recréés sur la cible et suivre la procédure Migrer les magasins d'identités. Pour plus d'informations, reportez-vous à la section [Migrer des magasins d'identités vers VMware Identity Manager](#).

Conditions préalables

- [Collecter les informations requises pour la migration.](#)
- [Obtenir la clé de chiffrement à partir de l'environnement vRealize Automation source.](#)
- [Ajouter chaque locataire à l'environnement cible à partir de l'environnement source de vRealize Automation.](#)
- [Créer un administrateur pour chaque locataire ajouté.](#)
- [Synchroniser les utilisateurs et les groupes pour un lien Active Directory avant la migration vers un environnement minimal.](#)

- [Cloner manuellement la base de données Microsoft SQL vRealize AutomationIaaS source.](#)
- [Snapshot de l'environnement vRealize Automation cible.](#)
- Connectez-vous à la gestion des dispositifs vRealize Automation cible en tant qu'**utilisateur racine** à l'aide du mot de passe que vous avez entré lorsque vous avez déployé le dispositif vRealize Automation cible.

Procédure

- 1 Sélectionnez **Migrer**.
- 2 Entrez les informations du dispositif vRealize Automation source.

Option	Description
Nom d'hôte	Nom d'hôte du dispositif vRealize Automation source.
Nom d'utilisateur racine	root
Mot de passe racine	Mot de passe de l'utilisateur racine que vous avez entré lorsque vous avez déployé le dispositif vRealize Automation.
Emplacement du module de migration	Chemin d'accès à un répertoire existant sur le dispositif vRealize Automation source sur lequel le module de migration est créé.

- 3 Entrez les informations du dispositif vRealize Automation cible.

Option	Description
Nom d'utilisateur racine	root
Mot de passe racine	Mot de passe de l'utilisateur racine que vous avez entré lorsque vous avez déployé le dispositif vRealize Automation cible.
Locataire par défaut	vsphere.local Vous ne pouvez pas modifier ce champ.
Nom d'utilisateur de l'administrateur	administrateur Vous ne pouvez pas modifier ce champ.
Mot de passe de l'administrateur	Mot de passe de l'utilisateur administrator@vsphere.local que vous avez entré lors du déploiement de l'environnement vRealize Automation cible.

4 Entrez les informations pour le serveur de base de données IaaS cible.

Option	Description
Serveur de base de données	Emplacement de l'instance de Microsoft SQL Server dans laquelle réside la base de données Microsoft SQL vRealize Automation IaaS restaurée. Si une instance nommée et un port autre que le port par défaut sont utilisés, entrez l'option au format <i>SERVER,PORT\INSTANCE-NAME</i> . Si vous configurez la cible de Microsoft SQL Server pour utiliser la fonctionnalité Groupe de disponibilité AlwaysOn (AAG), la cible SQL Server doit être entrée comme le nom de l'écouteur AAG, sans un nom de port ou d'instance.
Nom de la base de données clonée	Nom de la base de données vRealize Automation IaaS Microsoft SQL source que vous avez sauvegardée sur la source et restaurée sur l'environnement cible.
Mode d'authentification	<ul style="list-style-type: none"> ■ Windows Si vous utilisez le mode d'authentification Windows, l'utilisateur du service IaaS doit avoir le rôle db_owner dans SQL Server. Les mêmes autorisations s'appliquent lors de l'utilisation du mode d'authentification SQL Server. ■ SQL Server SQL Server ouvre les zones de texte Nom de connexion et Mot de passe.
Nom de connexion	Nom de connexion de l'utilisateur de SQL Server ayant le rôle db_owner pour la base de données Microsoft SQL IaaS clonée.
Mot de passe	Mot de passe de l'utilisateur de SQL Server ayant le rôle db_owner pour la base de données Microsoft SQL IaaS clonée.
Clé de chiffrement d'origine	Clé de chiffrement d'origine que vous récupérez depuis l'environnement source. Reportez-vous à Obtenir la clé de chiffrement à partir de l'environnement vRealize Automation source .
Nouvelle phrase secrète	Série de mots utilisés pour générer une nouvelle clé de chiffrement. Vous utilisez cette phrase secrète chaque fois que vous installez un nouveau composant IaaS dans l'environnement vRealize Automation cible.

5 Cliquez sur **Valider**.

La page affiche l'avancement de la validation.

- Si la validation d'un élément échoue, vérifiez le message d'erreur et le fichier journal de validation sur les nœuds IaaS. Pour les emplacements des fichiers journaux, reportez-vous à la section [Emplacements des journaux de migration](#). Cliquez sur **Modifier les paramètres** et modifiez l'élément à l'origine du problème.

6 Cliquez sur **Migrer**.

La page affiche l'avancement de la migration.

- Si la migration réussit, la page affiche toutes les tâches de migration comme étant terminées.

- Si la migration échoue, examinez les fichiers journaux de migration sur le dispositif virtuel et les nœuds IaaS. Pour les emplacements des fichiers journaux, reportez-vous à la section [Emplacements des journaux de migration](#).

Terminez les étapes suivantes avant de redémarrer la migration.

- a Restaurez votre environnement vRealize Automation cible à l'état que vous avez capturé lorsque vous avez pris un snapshot avant la migration.
- b Restaurez votre base de données IaaS Microsoft SQL cible à l'aide de la sauvegarde de la base de données IaaS source.

Étape suivante

Tâches post-migration.

Migrer les données source vRealize Automation vers un environnement vRealize Automation à haute disponibilité

Vous pouvez migrer les données de votre environnement vRealize Automation actuel vers une nouvelle version de vRealize Automation configurée en tant qu'environnement à haute disponibilité.

Tous les locataires du système source doivent être recréés sur la cible et suivre la procédure Migrer les magasins d'identités. Pour plus d'informations, reportez-vous à la section [Migrer des magasins d'identités vers VMware Identity Manager](#).

Conditions préalables

- [Collecter les informations requises pour la migration](#).
- [Obtenir la clé de chiffrement à partir de l'environnement vRealize Automation source](#).
- [Ajouter chaque locataire à l'environnement cible à partir de l'environnement source de vRealize Automation](#).
- [Créer un administrateur pour chaque locataire ajouté](#).
- [Synchroniser les utilisateurs et les groupes pour un lien Active Directory avant la migration vers un environnement à haute disponibilité](#).
- [Cloner manuellement la base de données Microsoft SQL vRealize Automation IaaS source](#).
- [Snapshot de l'environnement vRealize Automation cible](#).
- Connectez-vous à la gestion des dispositifs vRealize Automation cible en tant qu'**utilisateur racine** à l'aide du mot de passe que vous avez entré lorsque vous avez déployé le dispositif vRealize Automation cible.

Procédure

- 1 Sélectionnez **Migrer**.

2 Entrez les informations du dispositif vRealize Automation source.

Option	Description
Nom d'hôte	Nom d'hôte du dispositif vRealize Automation source.
Nom d'utilisateur racine	root
Mot de passe racine	Mot de passe de l'utilisateur racine que vous avez entré lorsque vous avez déployé votre dispositif vRealize Automation source.

3 Entrez les informations d'emplacement du module de migration sur le dispositif vRealize Automation source.

Option	Description
Emplacement du module de migration	Chemin d'accès à un répertoire existant sur le dispositif vRealize Automation source sur lequel le module de migration est créé.

4 Entrez les informations du dispositif vRealize Automation cible.

Option	Description
Nom d'utilisateur racine	root
Mot de passe racine	Mot de passe de l'utilisateur racine que vous avez entré lorsque vous avez déployé le dispositif vRealize Automation cible.
Locataire par défaut	vsphere.local
Nom d'utilisateur de l'administrateur	administrateur
Mot de passe de l'administrateur	Mot de passe de l'utilisateur administrator@vsphere.local que vous avez entré lors du déploiement de l'environnement vRealize Automation cible.

5 Entrez les informations pour le serveur de base de données IaaS cible.

Option	Description
Serveur de base de données	Emplacement de l'instance de Microsoft SQL Server dans laquelle réside la base de données Microsoft SQL vRealize AutomationIaaS restaurée. Si une instance nommée et un port autre que le port par défaut sont utilisés, entrez l'option au format <i>SERVER,PORT\INSTANCE-NAME</i> . Si vous configurez la cible de Microsoft SQL Server pour utiliser la fonctionnalité Groupe de disponibilité AlwaysOn (AAG), la cible SQL Server doit être entrée comme le nom de l'écouteur AAG, sans un nom de port ou d'instance.
Nom de la base de données clonée	Nom de la base de données vRealize AutomationIaaS Microsoft SQL source que vous avez sauvegardée sur la source et restaurée sur l'environnement cible.

Option	Description
Mode d'authentification	<ul style="list-style-type: none"> ■ Windows Si vous utilisez le mode d'authentification Windows, l'utilisateur du service IaaS doit avoir le rôle db_owner dans SQL Server. Les mêmes autorisations s'appliquent lors de l'utilisation du mode d'authentification SQL Server. ■ SQL Server SQL Server ouvre les zones de texte Nom de connexion et Mot de passe.
Nom de connexion	Nom de connexion de l'utilisateur de SQL Server ayant le rôle db_owner pour la base de données Microsoft SQL IaaS clonée.
Mot de passe	Mot de passe de l'utilisateur de SQL Server ayant le rôle db_owner pour la base de données Microsoft SQL IaaS clonée.
Clé de chiffrement d'origine	Clé de chiffrement d'origine que vous récupérez depuis l'environnement source. Reportez-vous à Obtenir la clé de chiffrement à partir de l'environnement vRealize Automation source .
Nouvelle phrase secrète	Série de mots utilisés pour générer une nouvelle clé de chiffrement. Vous utilisez cette phrase secrète chaque fois que vous installez un nouveau composant IaaS dans l'environnement vRealize Automation cible.

6 Cliquez sur **Valider**.

La page affiche l'avancement de la validation.

- Si la validation d'un élément échoue, vérifiez le message d'erreur et le fichier journal de validation sur les nœuds IaaS. Pour les emplacements des fichiers journaux, reportez-vous à la section [Emplacements des journaux de migration](#). Cliquez sur **Modifier les paramètres** et modifiez l'élément à l'origine du problème.

7 Cliquez sur **Migrer**.

La page affiche l'avancement de la migration.

- Si la migration réussit, la page affiche toutes les tâches de migration comme étant terminées.
- Si la migration échoue, examinez les fichiers journaux de migration sur le dispositif virtuel et les nœuds IaaS. Pour les emplacements des fichiers journaux, reportez-vous à la section [Emplacements des journaux de migration](#).

Terminez les étapes suivantes avant de redémarrer la migration.

- Restaurer votre environnement vRealize Automation cible à l'état que vous avez capturé lorsque vous avez pris un snapshot avant la migration.
- Restaurer votre base de données Microsoft SQL IaaS cible en utilisant la sauvegarde de la base de données IaaS source.

Étape suivante

[Tâches post-migration](#).

Tâches post-migration

Après la migration de vRealize Automation, effectuez les tâches post-migration applicables à votre situation.

Note Après la migration des magasins d'identités, les utilisateurs de vRealize Code Stream doivent manuellement réattribuer des rôles vRealize Code Stream.

Ne pas modifier le fuseau horaire vRealize Automation

Même si l'interface de gestion du dispositif vRealize Automation fournit une option pour la modifier, laissez toujours le fuseau horaire vRealize Automation défini sur Etc/UTC.

L'utilisation d'un fuseau horaire autre qu'Etc/UTC peut provoquer des erreurs inhabituelles telles que l'échec de migrations et des bundles de journaux qui ne contiennent pas les entrées provenant de tous les nœuds vRealize Automation.

L'option de l'interface de gestion du dispositif vRealize Automation que vous devez éviter se trouve sous **Système > Fuseau horaire**.

Ajouter des administrateurs de locataires et des administrateurs IaaS à partir de l'environnement vRealize Automation 6.2.x source

Vous devez supprimer et restaurer les administrateurs de locataires de vRealize Automation 6.2.x dans chaque locataire après la migration.

Procédez comme suit pour chaque locataire dans la console vRealize Automation cible.

Note Si vous effectuez la migration depuis un environnement vRealize Automation 7.x, vous pouvez ignorer cette procédure.

Conditions préalables

- Migration vers la dernière version de vRealize Automation réussie.
- Connectez-vous à la console vRealize Automation cible en tant qu'**administrateur** avec le mot de passe que vous avez entré lorsque vous avez déployé le dispositif vRealize Automation cible.

Procédure

- 1 Sélectionnez **Administration > Locataires**.
- 2 Cliquez sur le nom d'un locataire.
- 3 Cliquez sur **Administrateurs**.
- 4 Créez une liste des noms des administrateurs de locataires et des utilisateurs.
- 5 Pointez chaque administrateur et cliquez sur l'icône de suppression (Supprimer) jusqu'à ce que vous ayez supprimé tous les administrateurs.
- 6 Cliquez sur **Terminer**.
- 7 Sur la page Locataires, cliquez de nouveau sur le nom du locataire.

8 Cliquez sur **Administrateurs**.

9 Entrez le nom de chaque utilisateur que vous avez supprimé dans la zone de recherche appropriée et appuyez sur Entrée.

10 Cliquez sur le nom de l'utilisateur approprié dans les résultats de la recherche pour ajouter l'utilisateur en tant qu'administrateur.

Lorsque vous avez terminé, la liste des administrateurs de locataires ressemble à la liste des administrateurs que vous avez supprimée.

11 Cliquez sur **Terminer**.

Exécuter l'action Tester la connexion et vérifier les points de terminaison migrés

La migration de vRealize Automation apporte des modifications aux points de terminaison dans l'environnement vRealize Automation cible.

Après la migration de vRealize Automation, vous devez utiliser l'action **Tester la connexion** pour tous les points de terminaison applicables. Vous devrez également ajuster certains points de terminaison migrés. Pour plus d'informations, reportez-vous à la section [Considérations lors de l'utilisation de points de terminaison mis à niveau ou migrés](#).

Le paramètre de sécurité par défaut pour les points de terminaison mis à niveau ou migrés consiste à ne pas accepter les certificats non approuvés.

Après la mise à niveau ou la migration à partir d'une version antérieure à vRealize Automation, si vous utilisez des certificats non approuvés, vous devez effectuer la procédure suivante pour tous les points de terminaison vSphere et NSX afin d'activer la validation du certificat. Si vous ne le faites pas, les opérations de point de terminaison échouent et produisent des erreurs de certificat. Pour plus d'informations, consultez les articles de la base de connaissances VMware *La communication au point de terminaison est interrompue après la mise à niveau vers vRA 7.3* (2150230) à l'adresse <http://kb.vmware.com/kb/2150230> et *Comment télécharger et installer des certificats vCenter Server racine pour éviter les avertissements de certificat de navigateur Web* (2108294) à l'adresse <http://kb.vmware.com/kb/2108294>.

1 Après une mise à niveau ou une migration, connectez-vous à la machine de l'agent vSphere/vRealize Automation et redémarrez vos agents vSphere à l'aide de l'onglet **Services**.

Il se peut que la migration ne fasse pas redémarrer tous les agents ; si tel est le cas, redémarrez-les manuellement.

2 Attendez qu'au moins un rapport de commande ping se termine. Cette opération peut prendre une à deux minutes.

3 Lorsque les agents vSphere ont démarré la collecte de données, connectez-vous à vRealize Automation en tant qu'administrateur laaS.

4 Cliquez sur **Infrastructure > Points de terminaison > Points de terminaison**.

5 Modifiez un point de terminaison vSphere et cliquez sur **Tester la connexion**.

6 Si une invite de certificat s'affiche, cliquez sur **OK** pour accepter le certificat.

Si aucune invite de certificat ne s'affiche, il se peut qu'actuellement le certificat soit correctement stocké dans une autorité racine approuvée du service d'hébergement de la machine Windows pour le point de terminaison, par exemple en tant que machine de l'agent proxy ou machine DEM.

- 7 Cliquez sur **OK** pour appliquer l'acceptation du certificat et enregistrer le point de terminaison.
- 8 Répétez cette procédure pour chaque point de terminaison vSphere.
- 9 Répétez cette procédure pour chaque point de terminaison NSX.
- 10 Accédez à **Infrastructure > Ressources de calcul**, cliquez avec le bouton droit sur votre ressource **vCenter Compute**, puis exécutez **Collecte de données**.

Si l'action **Tester la connexion** réussit, mais certaines opérations de collecte ou de provisionnement de données échouent, vous pouvez installer le même certificat sur toutes les machines de l'agent qui servent de point de terminaison et sur toutes les machines DEM. Vous pouvez également désinstaller le certificat des machines existantes et répéter la procédure précédente pour le point de terminaison défaillant.

Exécuter la collecte de données d'inventaire réseau et de sécurité NSX dans votre environnement vRealize Automation cible

Après la migration, vous devez exécuter la collecte de données d'inventaire réseau et de sécurité NSX dans l'environnement vRealize Automation cible.

Cette collecte de données est nécessaire pour que l'action de reconfiguration de l'équilibrage de charge fonctionne dans l'environnement vRealize Automation cible après la migration.

Note Vous n'avez pas besoin d'effectuer cette collecte de données si vous avez réalisé la migration à partir de vRealize Automation 6.2.x.

Conditions préalables

- [Exécuter la collecte de données réseau et de sécurité NSX dans l'environnement vRealize Automation source](#).
- Migration réussie vers l'environnement vRealize Automation cible

.

Procédure

- ◆ Exécutez la collecte de données d'inventaire réseau et de sécurité NSX dans votre environnement vRealize Automation cible avant de migrer vers vRealize Automation. Reportez-vous à la section [Démarrer la collecte de données de point de terminaison manuellement](#) dans *Gestion de vRealize Automation*.

Reconfigurer les équilibres de charge après la migration vers un environnement à haute disponibilité

Lorsque vous migrez vers un environnement à haute disponibilité, vous devez effectuer ces tâches pour chaque équilibre de charge une fois la migration terminée.

Conditions préalables

[Migrer les données source vRealize Automation vers un environnement vRealize Automation à haute disponibilité.](#)

Procédure

- 1 Restaurez les paramètres de contrôle de santé d'origine afin que les nœuds de réplica puissent accepter le trafic entrant en configurant les équilibres de charge pour ces éléments.
 - Dispositif vRealize Automation.
 - Serveur Web IaaS qui héberge Model Manager.
 - Manager Service.
- 2 Rétablissez les paramètres de délai d'expiration d'équilibre de charge à la valeur par défaut.

Migration d'un serveur vRealize Orchestrator externe vers la version cible de vRealize Automation

Vous pouvez migrer votre serveur vRealize Orchestrator externe existant vers une instance de vRealize Orchestrator intégrée à vRealize Automation.

Conditions préalables

Migration réussie vers la version cible de vRealize Automation.

Pour plus d'informations, reportez-vous à la section *Migration d'un serveur Orchestrator externe vers vRealize Automation* dans la [documentation du produit vRealize Orchestrator](#).

Reconfigurer le point de terminaison vRealize Automation dans le dispositif vRealize Orchestrator cible

Utilisez la procédure suivante pour reconfigurer le point de terminaison vRealize Automation dans le dispositif vRealize Orchestrator cible intégré.

Conditions préalables

- Migration vers la dernière version de vRealize Automation réussie.
- Connectez-vous au dispositif vRealize Orchestrator cible à l'aide du client vRealize Orchestrator. Pour plus d'informations, reportez-vous à la section *Travailler avec VMware vRealize Orchestrator Client* dans la [documentation de vRealize Orchestrator](#).

Procédure

- 1 Sélectionnez l'option **Conception** dans le menu déroulant supérieur.

2 Cliquez sur **Inventaire**.

3 Développez **vRealize Automation**.

4 Si vous avez effectué une migration à partir d'un environnement minimal, identifiez les points de terminaison contenant le nom de domaine complet (FQDN) de l'hôte du dispositif vRealize Automation source. Si vous avez effectué une migration à partir d'un environnement à haute disponibilité, identifiez les points de terminaison contenant le nom de domaine complet de l'équilibrage de charge du dispositif source.

Si vous trouvez des points de terminaison contenant le nom de domaine complet, procédez comme suit.	Si vous ne trouvez aucun point de terminaison contenant le nom de domaine complet, procédez comme suit.
<ol style="list-style-type: none"> 1 Cliquez sur Workflows. 2 Cliquez sur le bouton de développement pour sélectionner Bibliothèque > vRealize Automation > Configuration. 3 Effectuez l'une des étapes suivantes. <ul style="list-style-type: none"> ■ Si vous avez effectué une migration à partir d'un environnement minimal, exécutez le workflow Supprimer un hôte vRA pour chaque point de terminaison contenant le nom de domaine complet de l'hôte du dispositif vRealize Automation source. ■ Si vous avez effectué la migration à partir d'un environnement à haute disponibilité, exécutez le workflow Supprimer un hôte vRA pour chaque point de terminaison contenant le nom de domaine complet de l'équilibrage de charge du dispositif source. 	<ol style="list-style-type: none"> 1 Cliquez sur Ressources. 2 Cliquez sur l'icône de mise à jour dans la barre d'outils supérieure. 3 Cliquez sur le bouton de développement pour sélectionner Bibliothèque > vCACCAFE > Configuration. 4 Effectuez l'une des étapes suivantes. <ul style="list-style-type: none"> ■ Si vous avez effectué une migration à partir d'un environnement minimal, supprimez chaque ressource disposant d'une propriété URL contenant le nom de domaine complet de l'hôte du dispositif vRealize Automation source. ■ Si vous avez effectué une migration à partir d'un environnement à haute disponibilité, supprimez chaque ressource disposant d'une propriété URL contenant le nom de domaine complet de l'équilibrage de charge du dispositif vRealize Automation source.

5 Cliquez sur **Workflows**.

6 Cliquez sur le bouton de développement pour sélectionner **Bibliothèque > vRealize Automation > Configuration**.

7 Pour ajouter l'hôte du dispositif vRealize Automation cible ou, si vous avez migré vers un déploiement à haute disponibilité, l'hôte équilibré en charge, exécutez le workflow **Ajouter un hôte vRA à l'aide du registre de composants**.

Reconfigurer le point de terminaison d'infrastructure vRealize Automation dans le dispositif vRealize Orchestrator cible

Utilisez la procédure suivante pour reconfigurer le point de terminaison d'infrastructure vRealize Automation dans le dispositif vRealize Orchestrator cible intégré.

Conditions préalables

- Migration vers la dernière version de vRealize Automation réussie.

- Connectez-vous au dispositif vRealize Orchestrator cible à l'aide du client vRealize Orchestrator. Pour plus d'informations, reportez-vous à la section *Travailler avec VMware vRealize Orchestrator Client* dans la [documentation de vRealize Orchestrator](#).

Procédure

- 1 Sélectionnez l'option **Conception** dans le menu déroulant supérieur.
- 2 Cliquez sur **Inventaire**.
- 3 Développez l'option **Infrastructure vRealize Automation**.
- 4 Si vous avez effectué une migration à partir d'un environnement minimal, identifiez les points de terminaison contenant le nom de domaine complet (FQDN) de l'hôte de l'infrastructure vRealize Automation source. Si vous avez effectué une migration à partir d'un environnement à haute disponibilité, identifiez les points de terminaison contenant le nom de domaine complet de l'équilibrage de charge du dispositif source.

Si vous trouvez des points de terminaison contenant le nom de domaine complet, procédez comme suit.	Si vous ne trouvez aucun point de terminaison contenant le nom de domaine complet, procédez comme suit.
<ol style="list-style-type: none"> 1 Cliquez sur Workflows. 2 Cliquez sur le bouton de développement pour sélectionner Bibliothèque > vRealize Automation > Administration d'infrastructure > Configuration. 3 Effectuez l'une des étapes suivantes. <ul style="list-style-type: none"> ■ Si vous avez effectué une migration à partir d'un environnement minimal, exécutez le workflow Supprimer un hôte IaaS pour chaque point de terminaison contenant le nom de domaine complet de l'hôte d'infrastructure vRealize Automation source. ■ Si vous avez effectué la migration à partir d'un environnement à haute disponibilité, exécutez le workflow Supprimer un hôte IaaS pour chaque point de terminaison contenant le nom de domaine complet de l'équilibrage de charge de l'hôte d'infrastructure vRealize Automation source. 	<ol style="list-style-type: none"> 1 Cliquez sur Ressources. 2 Cliquez sur l'icône de mise à jour dans la barre d'outils supérieure. 3 Cliquez sur le bouton de développement pour sélectionner Bibliothèque > vCAC > Configuration. 4 Effectuez l'une des étapes suivantes. <ul style="list-style-type: none"> ■ Si vous avez effectué une migration à partir d'un environnement minimal, supprimez chaque ressource disposant d'une propriété host contenant le nom de domaine complet de l'hôte d'infrastructure vRealize Automation source. ■ Si vous avez effectué une migration à partir d'un environnement à haute disponibilité, supprimez chaque ressource disposant d'une propriété host contenant le nom de domaine complet de l'équilibrage de charge de l'hôte d'infrastructure vRealize Automation source.

- 5 Cliquez sur **Workflows**.
- 6 Cliquez sur le bouton de développement pour sélectionner **Bibliothèque > vRealize Automation > Configuration**.
- 7 Pour ajouter l'hôte d'infrastructure vRealize Automation cible ou, si vous avez migré vers un déploiement à haute disponibilité l'hôte équilibré en charge, exécutez le workflow **Ajouter l'hôte IaaS d'un hôte vRA**.

Installer une personnalisation de vRealize Orchestrator

Vous pouvez exécuter un workflow pour installer les stubs de workflow de modification d'état personnalisés et les workflows d'opérations de menu de vRealize Orchestrator.

Pour plus d'informations, reportez-vous à la section [Installer une personnalisation de vRealize Orchestrator](#).

Conditions préalables

Migration vers la dernière version de vRealize Automation réussie.

Reconfigurer le point de terminaison d'infrastructure vRealize Orchestrator intégré dans le dispositif vRealize Automation cible

Lorsque vous migrez depuis un environnement vRealize Automation 6.2.5, vous devez mettre à jour l'URL du point de terminaison d'infrastructure qui pointe vers le serveur vRealize Orchestrator intégré cible.

Conditions préalables

- Migrez vers vRealize Automation vers la version de vRealize Automation cible.
- Connectez-vous à la console vRealize Automation cible.
 - a Ouvrez la console vRealize Automation à l'aide du nom de domaine complet du dispositif virtuel cible : `https://vra-va-hostname.domain.name/vcac`.

Pour un environnement à haute disponibilité, ouvrez la console à l'aide du nom de domaine complet de l'équilibrage de charge du dispositif virtuel cible : `https://vra-va-lb-hostname.domain.name/vcac`.
 - b Connectez-vous en tant qu'utilisateur administrateur laaS.

Procédure

- 1 Sélectionnez **Infrastructure > Points de terminaison > Points de terminaison**.
- 2 Sur la page Points de terminaison, sélectionnez le point de terminaison vRealize Orchestrator, puis cliquez sur **Modifier**.
- 3 Dans la zone de texte Adresse, modifiez l'URL du point de terminaison vRealize Orchestrator.
 - Si vous avez migré vers un environnement minimal, remplacez l'URL du point de terminaison vRealize Orchestrator par `https://vra-va-hostname.domain.name:443/vco`.
 - Si vous avez migré vers un environnement à haute disponibilité, remplacez l'URL du point de terminaison vRealize Orchestrator par `https://vra-va-lb-hostname.domain.name:443/vco`.
- 4 Cliquez sur **OK**.

5 Exécutez manuellement une collecte de données sur le point de terminaison vRealize Orchestrator.

- a Sur la page Points de terminaison, sélectionnez le point de terminaison vRealize Orchestrator.
- b Sélectionnez **Actions > Collecte de données**.

Vérifiez que la collecte de données a réussi.

Reconfigurer le point de terminaison Microsoft Azure dans l'environnement vRealize Automation cible

Après la migration, vous devez reconfigurer votre point de terminaison Microsoft Azure.

Effectuez cette procédure pour chaque point de terminaison Microsoft Azure.

Conditions préalables

- Migration réussie vers la version cible de vRealize Automation.
- Connectez-vous à la console vRealize Automation cible.
 - a Ouvrez la console vRealize Automation à l'aide du nom de domaine complet du dispositif virtuel cible : `https://vra-va-hostname.domain.name/vcac`.

Pour un environnement à haute disponibilité, ouvrez la console à l'aide du nom de domaine complet de l'équilibrage de charge du dispositif virtuel cible : `https://vra-va-lb-hostname.domain.name/vcac`.
 - b Connectez-vous en tant qu'utilisateur administrateur IaaS.

Procédure

- 1** Sélectionnez **Administration > Configuration vRO > Points de terminaison**.
- 2** Sélectionnez un point de terminaison Microsoft Azure.
- 3** Cliquez sur **Modifier**.
- 4** Cliquez sur **Détails**.
- 5** Sélectionnez la région dans le menu déroulant de l'environnement Azure.
- 6** Entrez la clé secrète client d'origine dans la zone de texte correspondante.
- 7** Entrez l'URL de stockage dans la zone de texte URI du stockage Azure.
Exemple : `https://mystorageaccount.blob.core.windows.net`
- 8** Cliquez sur **Terminer**.
- 9** Répétez pour chaque point de terminaison Azure.

Migrer vRealize Automation Application Services 6.2.x

Vous pouvez utiliser l'outil de migration de VMware vRealize Automation Application Services pour migrer vos Blueprints de services d'application et vos profils de déploiement existants de VMware vRealize Application Services 6.2.x vers la version de vRealize Automation cible.

Conditions préalables

Migration vers la dernière version de vRealize Automation réussie.

Procédure

- ◆ Pour télécharger VMware vRealize Application Services Migration Tool, procédez comme suit.
 - a Cliquez sur [Télécharger VMware vRealize Automation](#).
 - b Sélectionnez **Pilotes et outils > VMware vRealize Application Services Migration Tool**.

Supprimer la base de données IaaS Microsoft SQL vRealize Automation cible d'origine

Vous pouvez supprimer la base de données IaaS d'origine une fois la migration terminée.

Conditions préalables

Migration vers la dernière version de vRealize Automation réussie.

Votre environnement migré n'utilise pas la base de données IaaS Microsoft SQL vRealize Automation d'origine créée lors de l'installation de l'environnement vRealize Automation cible. Vous pouvez supprimer cette base de données IaaS d'origine en toute sécurité à partir de Microsoft SQL Server après avoir terminé la migration.

Mettre à jour le contenu du menu Emplacement du centre de données après la migration

Après la migration, vous devez ajouter les emplacements de centre de données personnalisés manquants dans le menu déroulant **Emplacement**.

Après la migration vers la dernière version de vRealize Automation, les emplacements de centre de données dans le menu déroulant **Emplacement** de la page Ressources de calcul reviennent à la liste par défaut. Bien que des emplacements de centre de données personnalisés soient manquants, toutes les configurations de ressources de calcul migrent avec succès et la propriété `Vrm.DataCenter.Location` n'est pas affectée. Vous pouvez toujours ajouter des emplacements de centre de données personnalisés au menu **Emplacement**.

Conditions préalables

Migrez vers la dernière version de vRealize Automation.

Procédure

- ◆ Ajoutez les emplacements de centre de données manquants dans le menu déroulant **Emplacement**. Reportez-vous à la section [Scénario : ajouter des emplacements de centre de données pour les déploiements inter-région](#).

Mise à niveau des agents logiciels TLS 1.2

Après la migration de vRealize Automation, vous devez effectuer plusieurs tâches pour mettre à niveau les agents logiciels de votre environnement source vers Transport Layer Security (TLS) 1.2

À partir de vRealize Automation 7.4, TLS 1.2 est le seul protocole TLS pris en charge pour la communication des données entre vRealize Automation et votre navigateur. Après la migration, vous devez mettre à niveau les modèles de machine virtuelle existants à partir de votre environnement source vRealize Automation ainsi que toutes les machines virtuelles existantes.

Mettre à jour les modèles de machines virtuelles de l'environnement source

Vous devez mettre à jour les modèles vRealize Automation migrés existants après la migration afin que les agents logiciels utilisent le protocole TLS 1.2.

L'agent invité et le code de démarrage d'agent doivent être mis à jour dans les modèles de l'environnement source. Si vous utilisez une option de clone lié, vous devrez éventuellement remapper les modèles avec les machines virtuelles récemment créées et leurs snapshots.

Pour mettre à niveau vos modèles, effectuez les tâches suivantes :

- 1 Connectez-vous à vSphere.
- 2 Convertissez chaque modèle vRealize Automation migré en une machine virtuelle et mettez sous tension la machine.
- 3 Importez le programme d'installation du logiciel approprié et exécutez-le sur chaque machine virtuelle.
- 4 Convertissez à nouveau chaque machine virtuelle vers un modèle.

Utilisez cette procédure pour localiser les programmes d'installation de logiciels pour Linux ou Windows.

Conditions préalables

- Migration réussie de vRealize Automation 7.1x ou version ultérieure.
- [Appliquer le correctif de l'agent logiciel](#) si vous avez migré de vRealize Automation 7.1.x ou 7.3.x.

Procédure

- 1 Démarrez un navigateur et ouvrez la page de démarrage du dispositif vRealize Automation en utilisant le nom de domaine complet du dispositif virtuel : `https://vra-virtual-hostname.domain.name`.
- 2 Cliquez sur **Page d'invité et d'agents logiciels**.
- 3 Suivez les instructions des programmes d'installation de logiciels Linux ou Windows.

Étape suivante

[Identifier les machines virtuelles nécessitant une mise à niveau des agents logiciels.](#)

Identifier les machines virtuelles nécessitant une mise à niveau des agents logiciels

Vous pouvez utiliser le service de santé de la console vRealize Automation pour identifier les machines virtuelles qui nécessitent une mise à jour des agents logiciels vers TLS 1.2.

Il peut arriver que le correctif appliqué à votre environnement source vRealize Automation ne mette pas à niveau toutes les machines virtuelles. Vous pouvez utiliser le service de santé pour identifier les machines virtuelles qui nécessitent toujours une mise à jour des agents logiciels vers TLS 1.2. Tous les agents logiciels de l'environnement cible doivent être mis à jour pour permettre l'exécution des procédures de post-provisionnement.

Conditions préalables

- Migrez vRealize Automation 7.1.x ou version ultérieure.
- [Appliquer le correctif de l'agent logiciel](#) si vous avez migré de vRealize Automation 7.1.x ou 7.3.x.
- Connectez-vous à l'environnement de vRealize Automation cible sur le dispositif virtuel principal.

Procédure

- 1 Cliquez sur **Administration > Santé**.
- 2 Cliquez sur **Nouvelle configuration**.
- 3 Sur la page Détails de la configuration, fournissez les renseignements demandés.

Option	Commentaire
Nom	Entrez Vérification des agents logiciels .
Description	Ajoutez une description facultative, par exemple, Recherche des agents logiciels à mettre à niveau vers TLS 1.2 .
Produit	Sélectionnez le produit et la version cibles, par exemple vRealize Automation 7.4.0.
Planifier	Sélectionnez Aucun.

- 4 Cliquez sur **Suivant**.
- 5 Sur la page Sélectionner les suites de tests, sélectionnez **Tests système de vRealize Automation** et **Tests de locataire de vRealize Automation**.
- 6 Cliquez sur **Suivant**.

7 Sur la page Configurer les paramètres, fournissez les renseignements demandés.

Tableau 1-85. Dispositif virtuel vRealize Automation

Option	Description
Adresse du serveur Web public	<ul style="list-style-type: none"> ■ Pour un déploiement minimal, l'URL de base pour l'hôte du dispositif vRealize Automation. Par exemple, <code>https://va-host.domain/</code>. ■ Pour un déploiement haute disponibilité, l'URL de base de l'équilibrage de charge vRealize Automation. Par exemple, <code>https://load-balancer-host.domain/</code>.
Adresse de la console SSH	Nom de domaine complet du dispositif vRealize Automation. Par exemple, <code>va-host.domain</code> .
Utilisateur de la console SSH	root
Mot de passe de la console SSH	Mot de passe de l'utilisateur racine.
Temps de réponse maximal du service (ms)	Acceptez la valeur par défaut : 2 000

Tableau 1-86. Locataire système vRealize Automation

Option	Description
Administrateur du locataire système	administrateur
Mot de passe du locataire système	Mot de passe de l'administrateur.

Tableau 1-87. Surveillance de l'espace disque vRealize Automation

Option	Description
Pourcentage du seuil d'avertissement	Acceptez la valeur par défaut : 75
Pourcentage de seuil critique	Acceptez la valeur par défaut : 90

Tableau 1-88. Locataire vRealize Automation

Option	Description
Locataire en cours de test	Locataire sélectionné pour les tests.
Nom d'utilisateur administrateur Fabric	<p>Nom d'utilisateur administrateur Fabric. Par exemple, <code>admin@va-host.local</code>.</p> <p>Note Cet administrateur Fabric doit également disposer des rôles d'administrateur de locataire et d'administrateur IaaS pour pouvoir exécuter l'ensemble des tests.</p>
Mot de passe administrateur Fabric	Mot de passe administrateur Fabric.

8 Cliquez sur **Suivant**.

- 9 Sur la page Résumé, passez en revue les informations, puis cliquez sur **Terminer**.
La configuration de la vérification des agents logiciels est terminée.
- 10 Sur la carte de vérification des agents logiciels, cliquez sur **Exécuter**.
- 11 Lorsque le test est terminé, cliquez au centre de la carte de vérification des agents logiciels.
- 12 Sur la page de résultats de la vérification des agents logiciels, parcourez les résultats des tests et recherchez le test Rechercher la version des agents logiciels dans la colonne Nom. Si le résultat du test est Échec, cliquez sur le lien **Cause** dans la colonne Cause pour afficher les machines virtuelles qui comportent un agent logiciel obsolète.

Étape suivante

Si tel est le cas, reportez-vous à la section [Mettre à niveau les agents logiciels sur vSphere](#).

Mettre à niveau les agents logiciels sur vSphere

Après la migration, vous pouvez mettre à niveau tous les agents logiciels obsolètes sur vSphere vers TLS 1.2 à l'aide de la gestion des dispositifs vRealize Automation.

Cette procédure met à jour les agents logiciels obsolètes sur les machines virtuelles de votre environnement source vers TLS 1.2. Elle est requise pour effectuer la migration vers la version de vRealize Automation.

Conditions préalables

- [Appliquer le correctif de l'agent logiciel](#) si vous avez migré de vRealize Automation 7.1.x ou 7.3.x.
- Migration réussie de vRealize Automation 7.1.x ou version ultérieure.
- Vous avez utilisé le service de santé pour identifier les dispositifs virtuels comportant des agents logiciels obsolètes.

Procédure

- 1 Sur votre dispositif vRealize Automation principal, connectez-vous à la gestion des dispositifs vRealize Automation en tant qu'utilisateur **racine** à l'aide du mot de passe que vous avez entré lorsque vous avez déployé le dispositif vRealize Automation.

Pour un environnement haute disponibilité, ouvrez la gestion des dispositifs sur le dispositif principal.

- 2 Cliquez sur **vRA > Agents logiciels**.
- 3 Cliquez sur **Activer/désactiver TLS 1.0, 1.1**.

L'état de TLS v1.0, v1.1 est ACTIVÉ.

- 4 En ce qui concerne les informations d'identification du locataire, entrez les informations demandées pour le dispositif vRealize Automation source.

Option	Description
Nom du locataire	Nom du locataire sur le dispositif vRealize Automation source. Note L'utilisateur du locataire doit avoir le rôle d'architecte de logiciel.
Nom d'utilisateur	Nom d'utilisateur administrateur du locataire sur le dispositif vRealize Automation source.
Mot de passe	Mot de passe administrateur du locataire.

- 5 Cliquez sur **Tester la connexion**.

Si une connexion est établie, un message de réussite s'affiche.

- 6 Pour le dispositif source, entrez l'adresse IP ou le nom de domaine complet du dispositif vRealize Automation source.

Les dispositifs source et cible doivent utiliser les mêmes informations d'identification du locataire.

- 7 Cliquez sur **Répertorier les lots**.

Le tableau Liste de choix des lots apparaît.

- 8 Cliquez sur **Afficher**.

Un tableau apparaît avec une liste des machines virtuelles comportant des agents logiciels obsolètes.

- 9 Mettez à niveau l'agent logiciel des machines virtuelles présentant l'état **POUVANT ÊTRE MIS À NIVEAU**.

- Pour mettre à niveau l'agent logiciel d'une machine virtuelle individuelle, cliquez sur **Afficher** pour un groupe de machines virtuelles, identifiez la machine virtuelle que vous souhaitez mettre à niveau, puis cliquez sur **Exécuter** pour démarrer la mise à niveau.
- Pour mettre à niveau l'agent logiciel d'un lot de machines virtuelles, identifiez le groupe que vous souhaitez mettre à niveau, puis cliquez sur **Exécuter** pour démarrer la mise à niveau.

Si vous disposez de plus de 200 machines virtuelles à mettre à niveau, vous pouvez contrôler la vitesse de mise à niveau du lot en entrant des valeurs pour ces paramètres.

Option	Description
Taille du lot	Nombre de machines virtuelles sélectionnées pour la mise à niveau du lot. Vous pouvez modifier ce nombre pour régler la vitesse de mise à niveau.
Profondeur de file d'attente	Nombre d'exécutions parallèles de la mise à niveau qui s'exécutent en même temps. Par exemple, 20. Vous pouvez modifier ce nombre pour régler la vitesse de mise à niveau.
Erreurs du lot	Nombre d'erreurs REST entraînant le ralentissement de la mise à niveau du lot. Par exemple, si vous souhaitez arrêter la mise à niveau du lot en cours après 5 échecs afin d'améliorer la stabilité de la mise à niveau, entrez 5 dans le champ de texte.
Échecs du lot	Nombre d'échecs de mise à niveau des agents logiciels entraînant le ralentissement du traitement du lot. Par exemple, si vous souhaitez arrêter la mise à niveau du lot en cours après 5 échecs afin d'améliorer la stabilité de la mise à niveau, entrez 5 dans le champ de texte.
Interrogation du lot	Fréquence d'interrogation de la mise à niveau pour vérifier l'état du processus. Vous pouvez modifier ce nombre pour régler la vitesse de mise à niveau.

Si le processus de mise à niveau est trop lent ou génère trop de mises à niveau infructueuses, vous pouvez ajuster ces paramètres afin d'améliorer les performances de la mise à niveau.

Note Cliquer sur **Actualiser** permet d'effacer la liste des lots. Cela n'affecte rien le processus de mise à niveau. Cliquer sur **Actualiser** permet également d'actualiser les informations indiquant si TLS 1.2 est défini ou pas, mais aussi d'effectuer un contrôle de santé des services vRealize Automation. Si les services ne sont pas en cours d'exécution, un message d'erreur s'affiche et tous les autres boutons d'action sont désactivés.

10 Cliquez sur **Activer/désactiver TLS 1.0, 1.1**.

L'état de TLS v1.0, v1.1 est DÉSACTIVÉ.

Mettre à niveau les agents logiciels sur Amazon Web Service ou Microsoft Azure

Vous pouvez mettre à niveau manuellement les agents logiciels obsolètes sur Amazon Web Service (AWS) ou Microsoft Azure.

- Vous devez mettre à jour les propriétés de tunnel spécifiées dans la réservation du serveur vRealize Automation migré.

Note Remplacez toutes les instances des versions dans ces exemples par la version vRealize Automation de votre version cible.

Conditions préalables

- [Appliquer le correctif de l'agent logiciel](#) si vous avez migré de vRealize Automation 7.1.x ou 7.3.x.

- Migration réussie de vRealize Automation 7.1.x ou version ultérieure.
- Un tunnel de logiciel est présent et l'adresse IP du tunnel de la machine virtuelle est connue.

Procédure

- 1 Créez un fichier de nœud pour chaque nœud que vous devez mettre à niveau.

```
/usr/lib/vcac/server/webapps/ROOT/software/initializeUpdateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -tu <$TenantUser> -S <$SourceVRAServer>
```

- 2 Créez un fichier de plan pour mettre à niveau l'agent logiciel sur une machine virtuelle Linux ou Windows.

- Modifiez le fichier migrate params sous /var/log/vcac/agentupdate/{tenant}/{subtenant-UUID} afin qu'il contienne la valeur de l'adresse IP privée correspondant au point de terminaison Amazon AWS ou Microsoft Azure.

```
"key": "ipAddress",
  "value": {
    "type": "string",
    "value": "<$PrivateIp:$PrivatePort>"
  }
}
```

- Utilisez cette commande pour mettre à jour une machine Linux.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CL
Software.LinuxAgentUpdate74 --source_cloud_provider azure
```

- Utilisez cette commande pour mettre à jour une machine Windows.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CW
Software.WindowsAgentUpdate74 --source_cloud_provider azure
```

- Cette commande exécute le fichier de plan.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -tu <$TenantUser> --plan_file /usr/lib/vcac/server/
webapps/ROOT/software/plan
```

- 3 Utilisez-la pour mettre à jour l'agent logiciel au moyen du fichier de nœud de l'étape 1 et du fichier de plan de l'étape 2.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer> -t <$tenant> -tu <$TenantUser> --component_windows Software.WindowsAgentUpdate74 --component_linux Software.LinuxAgentUpdate74 --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --plan_index 0 --node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider azure --action plan_batch -S <$SourceVRAServer>
```

Vous pouvez aussi l'utiliser pour exécuter un seul nœud à la fois depuis le fichier de nœud en fournissant un index de nœud.

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <$DestinationVRAServer> -t <$tenant> -tu <$TenantUser> --component_windows Software.WindowsAgentUpdate74 --component_linux Software.LinuxAgentUpdate74 --plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --plan_index 0 --node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider azure --action execute_node -S <$SourceVRAServer> --node_index <0 through n-1>
```

Lorsque vous effectuez cette procédure, vous pouvez suivre les journaux provenant du dispositif virtuel vRealize Automation et de la machine hôte afin de voir le processus de mise à niveau des agents du serveur.

Après la mise à niveau, le processus de mise à niveau importe un script de mise à jour logicielle pour Windows ou Linux dans le dispositif virtuel vRealize Automation. Vous pouvez vous connecter à l'hôte du dispositif virtuel vRealize Automation pour vous assurer que le composant logiciel a été correctement importé. Une fois le composant importé, une mise à jour logicielle est envoyée à l'ancien service EBS (Event Broker Service) pour qu'il relaye les scripts de mise à jour logicielle aux machines virtuelles identifiées. Une fois la mise à niveau terminée et les nouveaux agents logiciels opérationnels, une liaison est établie avec le nouveau dispositif virtuel vRealize Automation via l'envoi d'une demande ping.

Note Fichiers journaux utiles

- Sortie Catalina de la source vRealize Automation : /var/log/vcac/catalina.out. Ce fichier affiche les demandes de mise à niveau effectuées au fur et à mesure de la migration des agents. Cette activité est identique à la demande de provisionnement d'un logiciel en cours d'exécution.
- Sortie Catalina de la destination vRealize Automation : /var/log/vcac/catalina.out. Ce fichier affiche les machines virtuelles migrées en indiquant leurs demandes ping avec les numéros de version 7.4.0-SNAPSHOT. Vous pouvez faire concorder ces informations en comparant les noms de rubrique EBS, par exemple, sw-agent-UUID.
- Dossier de mise à jour des agents sur le fichier journal de mise à niveau principal de la machine vRealize Automation de destination : /var/log/vmware/vcac/agentupdate/updateSoftwareAgents.log. Vous pouvez suivre ce fichier pour afficher les opérations de mise à niveau en cours.

- Journaux individuels disponibles sous les dossiers du locataire : `/var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}`. Les nœuds individuels y sont répertoriés en tant que fichiers du lot, avec les échecs et les extensions en cours.
- Machines virtuelles migrées : `/opt/vmware-appdirector/agent/logs/darwin*.log`. Vous pouvez vérifier cet emplacement de manière ponctuelle. Il doit indiquer les demandes de mises à jour logicielles en cours de réception ainsi que le redémarrage éventuel de l'agent de démarrage et de l'agent logiciel.

Modifier le paramètre du dictionnaire de propriétés après la migration depuis 6.2.5

Le contrôle `Label` dans le dictionnaire de propriétés de vRealize Automation 6.2.x n'existe pas dans le dictionnaire de propriétés de vRealize Automation 7.x.

Lors de la migration vers vRealize Automation 7.4 ou version antérieure, le contrôle `Label` est converti en un type de contrôle `TextBox` dans le dictionnaire de propriétés migrées.

Lors de la migration vers vRealize Automation 7.5 ou version ultérieure, le contrôle `Label` est converti en type de contrôle `TextArea` dans le dictionnaire de propriétés migrées. Le type de contrôle `TextArea` prend en charge des noms d'étiquette longs plus performants que le type de contrôle `TextBox` utilisé lors de la migration vers des versions antérieures de vRealize Automation 7.x.

Après la migration, vous pouvez définir des définitions de propriétés qui contiennent un type de contrôle `TextBox` ou `TextArea` affecté comme non remplaçable, soit manuellement dans les paramètres des propriétés vRealize Automation de chaque Blueprint, manuellement dans chaque composant de Blueprint, réservation, point de terminaison, etc., dans lequel une définition de propriété personnalisée affectée est utilisée, ou par programmation à l'aide des capacités d'exportation et d'importation de vRealize CloudClient.

Procédure

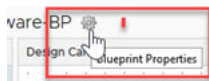
- 1 Après la migration et pour déterminer les définitions de propriétés qui utilisent un contrôle de type `Text Box` (7.4 et versions antérieures) ou `TextArea` (7.5 ou version ultérieure), cliquez sur **Administration > Définitions de propriétés** et affichez le paramètre **Zone d'affichage** pour chaque définition de propriété du type de données **Chaîne**.

Il s'agit des définitions de propriétés à définir comme ne devant pas être remplacées dans votre instance migrée de vRealize Automation.

- 2 Définissez les propriétés personnalisées affectées comme non remplaçables.

- Manuellement pour le Blueprint global

- 1 Cliquez sur l'onglet **Conception** et ouvrez un Blueprint.
- 2 Cliquez sur l'icône d'engrenage pour ouvrir la page **Propriétés du Blueprint**.



- 3 Cliquez sur l'onglet **Propriétés** sur la page **Propriétés du Blueprint**, puis sur **Propriétés personnalisées**.
 - 4 Faites basculer le bouton **Remplaçable** pour toutes les définitions de propriétés qui contiennent un type de contrôle TextBox ou TextArea.
- Manuellement pour chaque composant de Blueprint, réservation, point de terminaison, etc., dans lequel une propriété personnalisée affectée est utilisée
 - 1 Pour les points de terminaison et la réservation, cliquez sur **Infrastructure** et sélectionnez **Points de terminaison** ou **Réservations**.
 - 2 Ouvrez chaque élément cible et utilisez son onglet Propriétés pour définir le contrôle de type Text Box (7.4 et versions antérieures) ou TextArea (7.5 ou version ultérieure) affecté comme non remplaçable.
 - 3 Ouvrez chaque Blueprint et utilisez l'onglet **Propriétés** de chaque machine, réseau et autre composant dans le canevas du Blueprint pour mettre à jour toutes les définitions de propriétés concernées.
 - Par programmation pour le Blueprint global
 - 1 Exportez le Blueprint en utilisant une séquence de commande d'exportation vRealize CloudClient.
 - 2 Marquez les définitions de propriétés concernées comme non remplaçables. Dans cet exemple, TestLabel est défini sur non remplaçable et TestOverrideLabel est défini de manière à pouvoir être modifié sur un formulaire de demande.

```
TestLabel:
  fixed: default test label description at BP
  required: true
  secured: false
  visible: true
TestOverrideLabel:
  default: override this value
  required: true
  secured: false
  visible: true
```

- 3 Importez le Blueprint à l'aide d'une séquence de commande d'importation vRealize CloudClient.

Valider l'environnement vRealize Automation cible

Vous pouvez vérifier que toutes les données ont bien migré vers l'environnement vRealize Automation cible.

Conditions préalables

- Migrez vers la dernière version de vRealize Automation.

- Connectez-vous à la console vRealize Automation cible.
 - a Ouvrez la console vRealize Automation à l'aide du nom de domaine complet du dispositif virtuel cible : `https://vra-va-hostname.domain.name/vcac`.

Pour un environnement à haute disponibilité, ouvrez la console à l'aide du nom de domaine complet de l'équilibrage de charge du dispositif virtuel cible : `https://vra-va-lb-hostname.domain.name/vcac`.
 - b Connectez-vous avec le nom d'utilisateur et le mot de passe administrateur du locataire.

Procédure

- 1 Sélectionnez **Infrastructure > Machines gérées** et vérifiez que toutes les machines virtuelles gérées sont présentes.
- 2 Cliquez sur **Ressources de calcul**. Sélectionnez chaque point de terminaison et cliquez sur **Collecte de données**, **Demander maintenant** et **Actualiser** pour vérifier que les points de terminaison sont opérationnels.
- 3 Cliquez sur **Conception**, puis, sur la page **Blueprints**, sélectionnez et vérifiez les éléments de chaque Blueprint.
- 4 Cliquez sur **XaaS** et vérifiez le contenu de **Ressources personnalisées**, **Mappages de ressource**, **Blueprints XaaS** et **Actions sur les ressources**.
- 5 Sélectionnez **Administration > Gestion de catalogue**, puis vérifiez le contenu de **Services**, **Éléments du catalogue**, **Actions** et **Droits**.
- 6 Sélectionnez **Éléments > Déploiements** et vérifiez les détails des machines virtuelles provisionnées.
- 7 Sur la page Déploiements, sélectionnez une machine virtuelle provisionnée et hors tension, sélectionnez **Actions > Mettre sous tension**, puis cliquez sur **Envoyer** et sur **OK**. Vérifiez que la machine virtuelle se met bien sous tension.
- 8 Cliquez sur **Catalogue** et demandez un nouvel élément de catalogue.
- 9 Sur l'onglet **Général**, entrez les informations demandées.
- 10 Cliquez sur l'icône Machine, acceptez tous les paramètres par défaut, puis cliquez sur **Envoyer** et sur **OK**.
- 11 Vérifiez que la demande se termine correctement.

Restaurer les tables HF sur l'environnement vRealize Automation cible

Après la sauvegarde des tables HF sur votre environnement vRealize Automation cible et la migration vers vRealize Automation 7.x, vous devez restaurer les tables HF vers votre environnement cible.

Pour plus d'informations sur la sauvegarde des tables HF, reportez-vous à la section [Sauvegarder les tables HF sur l'environnement vRealize Automation cible](#).

Pour restaurer les tables HF dans votre environnement cible, copiez le fichier hf_tables.zip vers le nœud de destination sous /tmp/ et exécutez la commande :

```
cd /tmp
unzip ./hf_tables.zip -d ./hf_tables (ignore this command if hf_tables folder is already unzipped)
psql -U postgres -d vcac
\i /tmp/hf_tables/hf_patch.sql
\i /tmp/hf_tables/hf_patch_execution.sql
\i /tmp/hf_tables/hf_patch_nodes.sql
```

Dépannage de la migration

Les rubriques sur le dépannage de la migration apportent des solutions aux problèmes que vous pouvez rencontrer lorsque vous migrez vRealize Automation.

Erreur causée par la version de PostgreSQL

Un environnement vRealize Automation 6.2.x source contenant une base de données PostgreSQL mise à jour bloque l'accès de l'administrateur.

Problème

Si vRealize Automation 6.2.x utilise une base de données PostgreSQL mise à niveau, l'administrateur doit ajouter au fichier pg_hba.conf une entrée permettant d'accéder à cette base de données à partir de vRealize Automation.

Solution

- 1 Ouvrez le fichier pg_hba.conf.
- 2 Pour octroyer l'accès à cette base de données, ajoutez l'entrée suivante.

```
host all vcac-database-user vra-va-iptrust-method
```

Aucun déploiement n'est créé pour certaines machines virtuelles pendant la migration

Les machines virtuelles dont l'état indique qu'elles sont manquantes au moment de la migration n'ont pas de déploiement correspondant créé dans l'environnement cible.

Problème

Si l'état d'une machine virtuelle indique qu'elle est manquante dans l'environnement source pendant la migration, aucun déploiement correspondant n'est créé dans l'environnement cible.

Solution

- ◆ Si une machine virtuelle sort de l'état manquant après la migration, vous pouvez importer la machine virtuelle dans le déploiement cible à l'aide d'une importation en bloc.

La configuration de l'équilibrage de charge entraîne un délai d'expiration pour les opérations longues

La modification des paramètres de délai d'expiration de l'équilibrage de charge à 10 minutes peut ne pas empêcher un arrêt de connexion inattendu.

Problème

La définition du délai d'expiration à 10 minutes pour maintenir une connexion active pendant l'exécution d'une demande HTTP/HTTPS peut ne pas empêcher un arrêt de connexion inattendu lorsque la migration effectue des opérations longues.

Solution

- ◆ Si vous rencontrez un arrêt de connexion inattendu lors de la migration, augmentez la valeur du délai d'expiration de l'équilibrage de charge à plus de 10 minutes ou mettez à jour l'enregistrement DNS de l'équilibrage de charge pour qu'il pointe vers le nœud actif approprié pendant la durée de la migration. Une fois la migration terminée, rétablissez l'enregistrement DNS de l'équilibrage de charge.

Emplacements des journaux de migration

Vous pouvez résoudre les problèmes de validation ou de migration en consultant les journaux qui enregistrent le processus de migration.

Tableau 1-89. Dispositif vRealize Automation source

Journal	Emplacement
Journal de création du module	/var/log/vmware/vcac/migration-package.log

Tableau 1-90. Dispositif vRealize Automation cible

Journal	Emplacement
Journal de migration	/var/log/vmware/vcac/migrate.log
Journal d'exécution de la migration	/var/log/vmware/vcac/mseq.migration.log
Journal de sortie d'exécution de la migration	/var/log/vmware/vcac/mseq.migration.out.log
Journal d'exécution de la validation	/var/log/vmware/vcac/mseq.validation.log
Journal de sortie d'exécution de la validation	/var/log/vmware/vcac/mseq.validation.out.log

Tableau 1-91. Nœuds d'Infrastructure vRealize Automation cibles

Journal	Emplacement
Journal de migration	C:\Program Files (x86)\VMware\VCAC\InstallLogs-YYYYMMDDHHMMXX\Migrate.log
Journal de validation	C:\Program Files (x86)\VMware\VCAC\InstallLogs-YYYYMMDDHHMMXX\Validate.log

Les éléments de catalogue figurent dans le catalogue de services après la migration mais ne sont pas disponibles pour les demandes

Les éléments de catalogue qui utilisent certaines définitions de propriétés de versions précédentes figurent dans le catalogue de services, mais ne sont pas disponibles pour les demandes après la migration vers la dernière version de vRealize Automation.

Problème

Si vous avez procédé à la migration à partir de la version 6.2.x ou d'une version antérieure et que vous disposiez de définitions de propriétés avec ces types de contrôle ou attributs, ces attributs sont manquants dans les définitions de propriétés et les éléments de catalogue qui les utilisent ne fonctionnent plus comme avant la migration.

- Types de contrôle. Case à cocher ou lien.
- Attributs. Relation, expressions régulières ou dispositions de propriétés.

Cause

Dans vRealize Automation 7.0 et versions ultérieures, les définitions de propriétés n'utilisent plus ces éléments. Vous devez créer à nouveau la définition de propriété ou la configurer de façon à utiliser une action de script vRealize Orchestrator au lieu des types de contrôle ou d'attribut intégrés.

Procédez à la migration des types de contrôle ou des attributs vers vRealize Automation 7 à l'aide d'une action de script.

Solution

- 1 Dans vRealize Orchestrator, créez une action de script qui renvoie les valeurs des propriétés. L'action doit renvoyer un type simple. Par exemple, des chaînes, des entiers ou d'autres types d'éléments pris en charge. L'action peut utiliser les autres propriétés dont elle dépend en tant que paramètre d'entrée.
- 2 Dans la console vRealize Automation, configurez la définition de produit.
 - a Sélectionnez **Administration > Dictionnaire des propriétés > Définitions de propriétés**.
 - b Sélectionnez la définition de propriété, puis cliquez sur **Modifier**.
 - c Dans le menu déroulant Afficher un conseil, sélectionnez **Liste déroulante**.
 - d Dans le menu déroulant Valeurs, sélectionnez **Valeurs externes**.
 - e Sélectionnez l'action de script.
 - f Cliquez sur **OK**.
 - g Configurez les paramètres d'entrée inclus dans l'action de script. Pour conserver la relation existante, liez le paramètre à l'autre propriété.
 - h Cliquez sur **OK**.

Boutons radio de collecte de données désactivés dans vRealize Automation

Après la migration de vRealize Automation 6.2.x vers la version 7.x, la page Ressources de calcul sur l'instance de vRealize Automation cible contient des boutons radios désactivés sous Collecte de données.

Cause

Si vous installez un agent sur l'environnement source qui pointe vers un point de terminaison et installez un agent sur l'environnement cible qui pointe vers le même point de terminaison, mais que l'agent a un nom différent, vous pouvez exécuter un test de la connexion au point de terminaison en tant qu'administrateur dans l'environnement cible. Toutefois, si vous vous connectez à vRealize Automation sur l'environnement cible en tant qu'administrateur d'infrastructure, les boutons radio sous Collecte de données sur la page Ressources de calcul sont désactivés.

Solution

Pour éviter cette situation, attribuez à l'agent installé sur l'environnement cible le même nom que celui installé sur l'environnement source.

Dépannage de la mise à niveau de l'Agent logiciel

Lorsque vous utilisez la gestion de dispositifs vRealize Automation pour mettre à niveau les agents logiciels, vous pouvez vérifier les fichiers journaux pour identifier la cause des problèmes que vous rencontrez.

Problème

Vous pouvez rencontrer des problèmes lorsque vous mettez à niveau les agents logiciels. En observant les fichiers journaux lors du processus de mise à niveau de l'agent logiciel, vous pouvez identifier l'emplacement d'un problème éventuel.

Journaux du serveur

- Accédez à la fin du fichier `updateSoftwareAgents.log` sur le serveur pour observer le processus : `/storage/log/vmware/vcac/agentupdate/updateSoftwareAgents.log`.
- Accédez à la fin du fichier `catlaina.out` sur le dispositif cible pour voir quels agents logiciels réussissent : `/var/log/vcac/catalina.out`.

Recherchez les chaînes s telles que « ping » signalées pour *version.0-SNAPSHOT*.

Vous pouvez trouver des informations supplémentaires à ces emplacements.

- `/var/cache/vcac/agentupdate/{Tenant}/{UUID}/UUID.plan`
- `/var/cache/vcac/agentupdate/{Tenant}/{UUID}/UUID.log`
- `/var/cache/vcac/agentupdate/sqa/UUID/UUID.log` (selon le système d'exploitation)

Avant de commencer une mise à niveau majeure par traitement par lots, vous devez toujours effectuer une mise à niveau de test d'agent logiciel de dispositif virtuel. Pour obtenir un aperçu du processus :

- Observez la première demande adressée au dispositif virtuel cible afin d'identifier les versions d'agent.
- Observez la demande effectuée au dispositif virtuel source pour la mise à niveau.
- Observez les agents signalant leur nouvelle version dans le dispositif virtuel cible.
- Entre ces événements, observez le fichier `updateSoftwareAgents.log` à l'emplacement `/storage/log/vmware/vcac/agentupdate/updateSoftwareAgents.log`

Journaux du client

Les journaux de l'agent Linux se trouvent dans le dossier de journaux de l'agent appdirector : `/opt/vmware-appdirector/agent/logs/*.log`

Des journaux d'erreurs semblables à ceux-ci peuvent s'afficher, de manière temporaire, car les files d'attente EBS fluctuent pendant le processus de mise à niveau.

```
Feb 15 2018 16:54:10.105 ERROR [EventPoller-sw-agent-0ad2418d-5b42-4231-a839-a05dd618e43e] []
com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler - Error while
polling events for subscription '{}'
```

```
org.springframework.web.client.HttpClientErrorException: 404 Not Found
```

```
org.springframework.web.client.DefaultResponseErrorHandler.handleError(DefaultResponseErrorHa
ndler.java:91) ~[nobel-agent.jar:na]
```

```
org.springframework.web.client.RestTemplate.handleResponse(RestTemplate.java:641) ~[nobel-
agent.jar:na]
```

```
org.springframework.web.client.RestTemplate.doExecute(RestTemplate.java:597) ~[nobel-
agent.jar:na]
```

```
org.springframework.web.client.RestTemplate.execute(RestTemplate.java:557) ~[nobel-
agent.jar:na]
```

```
org.springframework.web.client.RestTemplate.exchange(RestTemplate.java:503) ~[nobel-
agent.jar:na]
```

```
com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler.pollEvents(RestEv
entSubscribeHandler.java:297) ~[nobel-agent.jar:na]
```

```
com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler
$EventPoller.run(RestEventSubscribeHandler.java:329) ~[nobel-agent.jar:na]
```

Scénarios de migration

Si vous migrez de vRealize Automation 6.2.5, vous pouvez rencontrer ces problèmes.

Problème dans la version 6.2.5	Résolution pour la dernière version
<p>Après la migration de vRealize Automation 6.2.5 vers la dernière version, les éléments de catalogue qui utilisent ces définitions de propriétés s'affichent dans le catalogue de services, mais ne sont pas disponibles pour les demandes.</p> <ul style="list-style-type: none"> ■ Types de contrôle : case à cocher ou lien. ■ Attributs : relation, expressions régulières ou dispositions de propriétés. <p>Dans la version de vRealize Automation, les définitions de propriété n'utilisent plus ces éléments.</p>	<p>Vous devez créer à nouveau la définition de propriété ou la configurer de façon à utiliser une action de script vRealize Orchestrator au lieu des types de contrôle ou d'attribut intégrés. Pour plus d'informations, reportez-vous à la section Les éléments de catalogue figurent dans le catalogue de services après la migration mais ne sont pas disponibles pour les demandes.</p>
<p>Les expressions régulières utilisées pour définir les relations parent-enfant dans un menu déroulant de vRealize Automation 6.2.5 ne sont pas prises en charge dans la version de vRealize Automation cible. Dans la version 6.2.5, vous pouvez utiliser des expressions régulières pour définir un ou plusieurs éléments de menu enfant qui sont uniquement disponibles pour un certain élément de menu parent. Seuls ces éléments de menu enfant s'affichent lorsque vous sélectionnez l'élément de menu parent.</p>	<p>Après la migration, vous devez recréer la définition de la propriété pour restaurer les valeurs dynamiques précédentes. Pour en savoir plus sur la création d'une relation parent-enfant entre le menu déroulant parent et le menu déroulant enfant, consultez Utilisation de définitions de propriété dynamique dans vRA 7.2.</p>
<p>Workflows vRealize Orchestrator utilisant des stubs de workflow</p>	<p>Les stubs de workflow peuvent être convertis en abonnements au service Broker d'événements après la migration.</p> <p>Pour plus d'informations sur les étapes de la conversion et les modifications, consultez le <i>Guide de migration d'extensibilité de vRealize Automation</i>.</p>
<p>Personnalisation des intégrations d'Active Directory</p>	<p>La configuration et les stratégies d'Active Directory sont intégrées dans le produit :</p> <p>Pour plus d'informations sur la configuration d'Active Directory, reportez-vous à Utilisation des stratégies Active Directory.</p>
<p>Configuration IPAM personnalisée pour les charges de travail provisionnées</p>	<p>La configuration IPAM est maintenant intégrée au produit. Pour plus d'informations sur les étapes de la configuration IPAM, reportez-vous à Liste de contrôle pour assurer la prise en charge d'un fournisseur IPAM tiers.</p>
<p>Utilisation du dictionnaire de propriétés d'expressions relationnelles</p>	<p>Les expressions relationnelles ne constituent plus un choix dans le dictionnaire des propriétés. L'exemple ci-dessous montre comment développer une relation de dictionnaire de propriétés dans la version 7.x :</p> <p>Relations de propriétés dans vRA 7</p>

Problème dans la version 6.2.5	Résolution pour la dernière version
Nom d'hôte personnalisé	Il existe différentes options pour l'attribution de noms d'hôtes personnalisés après la migration. Pour obtenir un aperçu de ces options, reportez-vous à Gérer les noms d'hôtes avec vRealize Automation - Partie 1 : comprendre vos options
Utilisation de Blueprints basés sur les services applicatifs	La migration de Blueprints basés sur les services applicatifs impose des étapes de migration distinctes. Pour plus d'informations sur les étapes de migration, reportez-vous au <i>Guide de l'utilisateur de l'outil VMware vRealize Application Services Migration Tool 1.1</i> .