

Gestion de vRealize Automation

21 juillet 2021

vRealize Automation 7.6

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 © 2015-2021 VMware, Inc. Tous droits réservés. [Informations relatives aux copyrights et marques commerciales.](#)

Table des matières

| | | |
|----------|---|----------|
| 1 | Maintenance et personnalisation des options et composants vRealize Automation | 5 |
| | Diffuser un message à tous les utilisateurs | 5 |
| | Créer une liste autorisée d'URL du panneau de messages | 7 |
| | Démarrage et arrêt de vRealize Automation | 8 |
| | Démarrage de vRealize Automation | 8 |
| | Redémarrer vRealize Automation | 9 |
| | Arrêter vRealize Automation | 11 |
| | Mise à jour de certificats vRealize Automation | 12 |
| | Extraction de certificats et de clés privées | 14 |
| | Remplacer des certificats dans le dispositif vRealize Automation | 14 |
| | Remplacer le certificat d'Infrastructure en tant que service | 17 |
| | Remplacer le certificat IaaS Manager Service | 19 |
| | Mettre à jour une instance intégrée de vRealize Orchestrator pour lui permettre d'approuver les certificats vRealize Automation | 21 |
| | Mettre à jour l'instance externe de vRealize Orchestrator pour qu'elle approuve les certificats vRealize Automation | 24 |
| | Mise à jour du certificat du site de gestion de dispositifs vRealize Automation | 24 |
| | Remplacer un certificat d'agent de gestion | 29 |
| | Modifier la méthode d'interrogation pour des certificats | 32 |
| | Gestion de la base de données de dispositif Postgres vRealize Automation | 33 |
| | Configurer la base de données du dispositif | 34 |
| | Scénarios de basculement automatique à trois nœuds de la base de données du dispositif | 36 |
| | Scénario : réaliser un basculement manuel de base de données de dispositif | 39 |
| | Scénario : réaliser un basculement de base de données de maintenance | 41 |
| | Récupérer manuellement la base de données de dispositif d'une défaillance irrémédiable | 42 |
| | Sauvegarde et récupération d'installations de vRealize Automation | 44 |
| | Programme d'amélioration de l'expérience utilisateur | 44 |
| | Rejoindre ou quitter le Programme d'amélioration du produit de vRealize Automation | 45 |
| | Configurer l'heure de collecte des données | 45 |
| | Ajustement des paramètres système | 46 |
| | Modifier l'icône Tous les services dans le catalogue de services | 46 |
| | Personnaliser les paramètres de rotation des données | 48 |
| | Ajustement des paramètres du fichier de configuration du service de gestionnaire | 50 |
| | Surveillance vRealize Automation | 56 |
| | Surveillance des workflows et affichage des journaux | 56 |
| | Surveillance des journaux d'événement et des services | 57 |

| | |
|--|----|
| Utilisation de la journalisation d'audit de vRealize Automation | 59 |
| Affichage des informations sur l'hôte pour les clusters dans des déploiements distribués | 61 |
| Surveillance de la santé de vRealize Automation | 63 |
| Configurez les tests système de vRealize Automation | 64 |
| Configurez les tests de locataire de vRealize Automation | 66 |
| Configuration des tests pour vRealize Orchestrator | 68 |
| Suite de tests personnalisés | 70 |
| Afficher les résultats de la suite de tests du service de santé vRealize Automation | 72 |
| Dépannage du service de santé | 72 |
| Surveillance des ressources d'environnement vRealize Automation à l'aide de SNMP | 73 |
| Surveillance et gestion des ressources | 74 |
| Choisir un scénario de surveillance des ressources | 74 |
| Terminologie de l'utilisation des ressources | 75 |
| Connexion à une machine de cloud | 76 |
| Réduction de l'utilisation de la réservation par attrition | 79 |
| Désaffectation d'un chemin de stockage | 80 |
| Collecte des données | 81 |
| Présentation de la vérification d'allocation vSwap pour les points de terminaison vCenter Server | 84 |
| Suppression de sites géographiques de centres de données | 85 |
| Surveillance des conteneurs | 86 |
| Importation, mise à jour ou migration de machines virtuelles en bloc | 86 |
| Importer une machine virtuelle dans un environnement vRealize Automation | 87 |
| Mettre à jour une machine virtuelle dans un environnement vRealize Automation | 92 |
| Migrer une machine virtuelle vers un autre environnement vRealize Automation | 95 |

Maintenance et personnalisation des options et composants vRealize Automation

1

Vous pouvez gérer des machines provisionnées et d'autres aspects de votre déploiement de vRealize Automation.

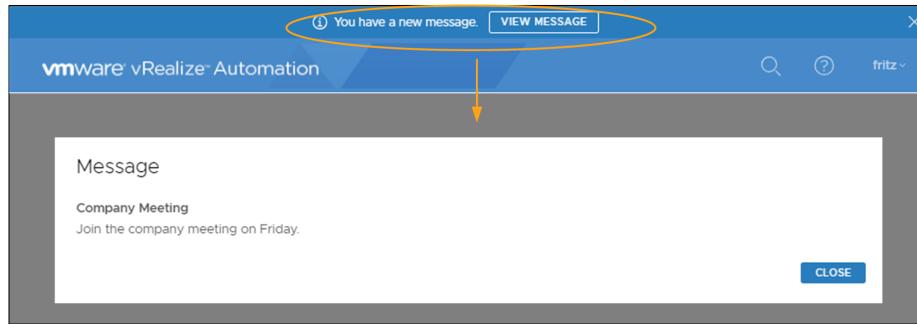
Ce chapitre contient les rubriques suivantes :

- [Diffuser un message à tous les utilisateurs](#)
- [Démarrage et arrêt de vRealize Automation](#)
- [Mise à jour de certificats vRealize Automation](#)
- [Gestion de la base de données de dispositif Postgres vRealize Automation](#)
- [Sauvegarde et récupération d'installations de vRealize Automation](#)
- [Programme d'amélioration de l'expérience utilisateur](#)
- [Ajustement des paramètres système](#)
- [Surveillance vRealize Automation](#)
- [Surveillance de la santé de vRealize Automation](#)
- [Surveillance des ressources d'environnement vRealize Automation à l'aide de SNMP](#)
- [Surveillance et gestion des ressources](#)
- [Surveillance des conteneurs](#)
- [Importation, mise à jour ou migration de machines virtuelles en bloc](#)

Diffuser un message à tous les utilisateurs

En tant qu'administrateur de locataire, vous pouvez diffuser un message à tous les utilisateurs. Les messages de notification s'affichent en haut de la page du navigateur. Vos utilisateurs cliquent sur la notification pour voir le message.

En tant qu'utilisateur, vous pouvez accéder au message à partir de la bannière, ou du menu déroulant utilisateur de l'en-tête.



Vous utilisez le Panneau de messages pour diffuser un message texte ou une page Web. Selon la page Web, vous utilisateurs peuvent naviguer sur le site Web dans le panneau de messages.

Le panneau de messages présente les limitations suivantes.

Tableau 1-1. Limitation du Panneau de messages

| Option | Limitations |
|--|--|
| Limitations des messages d'URL | <ul style="list-style-type: none"> ■ L'URL cible doit être incluse dans la liste autorisée du panneau de messages. Reportez-vous à Créer une liste autorisée d'URL du panneau de messages. ■ Vous pouvez uniquement publier du contenu qui est hébergé sur un site https. ■ Vous ne pouvez pas utiliser des certificats auto-signés. L'option permettant d'accepter le certificat ne figure pas dans le panneau de messages. ■ L'URL du panneau de messages est intégrée dans un iframe. Certains sites Web ne fonctionnent pas dans iframe et une erreur s'affiche. Une cause de l'échec est la présence de X-Frame-Options DENY ou SAMEORIGIN dans l'en-tête du site Web cible. Si votre site Web cible fait partie de ceux que vous contrôlez, vous pouvez définir l'en-tête X-Frame-Options sur X-Frame-Options: ALLOW-FROM https://<vRealizeAutomationApplianceURL>. ■ Certains sites Web ont une redirection vers une page de niveau supérieur qui peut actualiser toute la page vRealize Automation. Ce type de site Web ne fonctionne pas dans le panneau de messages. L'actualisation est supprimée et un message Chargement en cours... s'affiche sur le panneau de messages. ■ Si vous affichez une page HTML interne, la page ne peut pas utiliser l'hôte vRealize Automation comme URL. |
| Limitations des messages personnalisés | <ul style="list-style-type: none"> ■ Pour assurer la sécurité, le Message personnalisé permet le balisage simple, mais ne prend pas en charge le code HTML. Par exemple, vous ne pouvez pas utiliser l'attribut <href> pour effectuer une liaison vers un site Web. Vous devez utiliser l'option de message URL. |

Conditions préalables

Connectez-vous à vRealize Automation en tant qu'**administrateur de locataire**.

Procédure

- 1 Cliquez sur l'onglet **Administration**.
- 2 Sélectionnez **Notifications > Panneau de messages**
- 3 Dans le menu déroulant **Type**, sélectionnez le type de message.

| Option | Description |
|-----------------------------|---|
| Aucun | Supprime la notification de message. |
| Message personnalisé | Entrez un message en texte brut. |
| URL | Entrez l'URL de la page. L'URL doit être incluse dans la liste autorisée du panneau de messages. Reportez-vous à Créer une liste autorisée d'URL du panneau de messages . Pour connecter l'utilisateur à un site Web, le plus souvent votre site Web interne, en fonction de leur ID d'utilisateur vRealize Automation, sélectionnez Inclure ID d'utilisateur . L'URL qui est transmise au site Web similaire à <code>http://company.com/internal/message?userID=richard_dawson@company.com</code> . Cette méthode permet à votre site Web d'utiliser la propriété JavaScript <code>window.location.search</code> pour fournir des ID de l'utilisateur actuel à votre site Web. |

- 4 Cliquez sur **OK**.

Résultats

Le message est diffusé sous forme de bandeau à tous les utilisateurs de votre locataire.

Pour modifier ou supprimer le message, vous devez être connecté en tant qu'administrateur de locataire. Pour modifier le message, répétez la même procédure. Pour supprimer le message, sélectionnez **Aucun** comme Type et cliquez sur **OK**.

Créer une liste autorisée d'URL du panneau de messages

En tant qu'administrateur de sécurité, vous configurez une liste autorisée d'URL pouvant être utilisées dans le panneau de messages. Cette liste autorisée assure une sécurité accrue.

Conditions préalables

Connectez-vous à vRealize Automation en tant qu'**administrateur de sécurité**.

Procédure

- 1 Sélectionnez **Administration > Liste blanche du panneau de messages**.
- 2 Cliquez sur **Nouveau**.

3 Ajoutez une URL et cliquez sur **OK**.

Les entrées d'URL peuvent inclure le contenu suivant :

- Adresse IP ou nom de domaine complet d'un site. Par exemple, <https://docs.vmware.com>.
- Inclut https.
- Peut inclure des ports autorisés. Si un port n'est pas spécifié, les ports autorisés sont 80 et 443.

4 Répétez ces étapes pour chaque entrée supplémentaire.

Résultats

Un administrateur de locataire ne peut ajouter une URL au panneau de messages que si elle figure dans cette liste.

Étape suivante

Vérifiez que vous pouvez ajouter et diffuser une URL incluse dans votre liste autorisée en utilisant le panneau de messages. Reportez-vous à [Diffuser un message à tous les utilisateurs](#).

Démarrage et arrêt de vRealize Automation

Un administrateur système réalise un arrêt ou un démarrage contrôlé de vRealize Automation pour préserver l'intégrité des données et du système.

Vous pouvez également utiliser un arrêt ou un démarrage contrôlé pour résoudre des problèmes de performances et de comportement du produit pouvant découler d'un démarrage d'origine incorrect. Utilisez la procédure de redémarrage uniquement lorsque des composants de votre déploiement donnent lieu à un échec.

Démarrage de vRealize Automation

Lorsque vous démarrez vRealize Automation après la mise hors tension pour une raison attendue ou inattendue, vous devez démarrer les composants dans un ordre spécifique.

Si vous gérez des composants de déploiement dans vCenter Server, vous pouvez démarrer leurs systèmes d'exploitation invités à partir de cet emplacement.

Conditions préalables

Vérifiez que les équilibres de charge que votre déploiement utilise fonctionnent.

Procédure

- 1 Si vous utilisez une base de données PostgreSQL autonome héritée, démarrez ce serveur.
- 2 Dans n'importe quel ordre, démarrez les serveurs MS SQL vRealize Automation autonomes.
- 3 Dans un déploiement qui utilise des équilibres de charge avec des contrôles de santé, désactivez tous les contrôles de santé à l'exception des commandes ping.

- 4 Redémarrez le dispositif vRealize Automation principal.
 - 5 Dans l'interface de gestion du dispositif vRealize Automation principal, recherchez sous l'onglet **Cluster** si le système est en mode synchrone ou asynchrone. Un déploiement à un seul dispositif est toujours asynchrone.
 - Si le déploiement est synchrone, démarrez les dispositifs vRealize Automation restants.
 - Si le déploiement est asynchrone, accédez à l'interface de gestion du dispositif vRealize Automation principal et attendez que le service de licence soit en cours d'exécution et ENREGISTRÉ.

Ensuite, démarrez les dispositifs vRealize Automation restants.
 - 6 Une fois que tous les dispositifs ont démarré, utilisez leurs interfaces de gestion pour vérifier que les services sont en cours d'exécution et ENREGISTRÉS.
- Le démarrage des dispositifs peut prendre 15 minutes ou plus.
- 7 Démarrez tous les nœuds Web IaaS et attendez 5 minutes.
 - 8 Démarrez le nœud Manager Service principal et attendez 2 à 5 minutes.
 - 9 Dans un déploiement distribué avec plusieurs nœuds Manager Service, démarrez les nœuds Manager Service secondaires et attendez 2 à 5 minutes.
- Sur les machines secondaires, ne démarrez pas ou n'exécutez pas le service Windows, sauf si votre configuration prévoit le basculement automatique de Manager Service.
- 10 Dans n'importe quel ordre, démarrez l'orchestrateur DEM, les travailleurs DEM et tous les agents du proxy vRealize Automation.
- Vous n'avez pas besoin d'attendre qu'un démarrage se termine avant d'en démarrer un autre.
- 11 Si vous deviez désactiver les contrôles de santé de l'équilibrage de charge, réactivez-les.
 - 12 Vérifiez que les services démarrés fonctionnent et sont ENREGISTRÉS.
 - a Dans un navigateur, connectez-vous à l'interface de gestion du dispositif vRealize Automation principal.

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

 - b Cliquez sur l'onglet **Services**.
 - c Surveillez la progression du démarrage du service en cliquant sur **Actualiser**.

Résultats

Lorsque tous les services sont ENREGISTRÉS, le déploiement est prêt.

Redémarrer vRealize Automation

Le redémarrage des composants vRealize Automation peut aider à résoudre les problèmes. Vous devez redémarrer les composants dans un ordre spécifique.

Si vous gérez des composants de déploiement dans vCenter Server, vous pouvez redémarrer leurs systèmes d'exploitation invités à partir de cet emplacement.

Si vous ne pouvez pas effectuer un redémarrage, essayez plutôt les instructions dans [Arrêter vRealize Automation](#) et [Démarrage de vRealize Automation](#).

Conditions préalables

- Vérifiez que tous les équilibres de charge que votre déploiement utilise sont en cours d'exécution.

Procédure

- 1 Vérifiez que la base de données du dispositif vRealize Automation fonctionne en mode asynchrone. Si nécessaire, utilisez l'interface de gestion pour passer en mode asynchrone. Vous pouvez revenir en mode synchrone après avoir terminé l'intégralité de la procédure. Consultez [Gestion de la base de données de dispositif Postgres vRealize Automation](#) pour plus d'informations.
- 2 Redémarrez le dispositif vRealize Automation principal et attendez la fin du démarrage.
- 3 Utilisez l'interface de gestion du dispositif vRealize Automation principal pour vérifier que le service de gestion des licences est en cours d'exécution et ENREGISTRÉ.
- 4 Redémarrez les dispositifs vRealize Automation restants simultanément.
- 5 Attendez que les dispositifs redémarrent et utilisez leur interface de gestion pour vérifier que les services sont en cours d'exécution et ENREGISTRÉS.

Le redémarrage des dispositifs peut prendre 15 minutes ou plus.

- 6 Redémarrez le nœud Web principal et attendez la fin du démarrage.
- 7 Si vous exécutez un déploiement distribué avec plusieurs nœuds Web, redémarrez tous les nœuds Web secondaires et attendez la fin des démarrages.
- 8 Redémarrez les nœuds de Manager Service et attendez la fin du démarrage.

Si vous exécutez un basculement automatique de Manager Service et que vous souhaitez conserver les nœuds actifs et passifs, redémarrez dans l'ordre suivant :

- a Arrêtez les nœuds Manager Service passifs sans les redémarrer.
- b Redémarrez complètement le nœud Manager Service actif.
- c Démarrez les nœuds Manager Service passifs.

- 9 Dans n'importe quel ordre, redémarrez l'orchestrateur DEM, les travailleurs DEM et tous les agents du proxy vRealize Automation. Attendez la fin de tous les démarrages.

Vous n'avez pas besoin d'attendre qu'un redémarrage se termine avant d'en redémarrer un autre.

10 Vérifiez que les services redémarrés fonctionnent et sont ENREGISTRÉS.

- a Dans un navigateur, connectez-vous à l'interface de gestion du dispositif vRealize Automation principal.

https://vrealize-automation-appliance-FQDN:5480
- b Cliquez sur l'onglet **Services**.
- c Surveillez la progression du démarrage du service en cliquant sur **Actualiser**.

Résultats

Lorsque tous les services sont ENREGISTRÉS, le déploiement est prêt.

Arrêter vRealize Automation

Pour préserver l'intégrité des données, vous devez arrêter vRealize Automation dans un ordre spécifique.

Si vous gérez des composants de déploiement dans vCenter Server, vous pouvez arrêter leurs systèmes d'exploitation invités à partir de cet emplacement.

Procédure

- 1** Dans n'importe quel ordre, arrêtez l'orchestrateur DEM, les travailleurs DEM et tous les agents du proxy vRealize Automation. Attendez la fin de l'arrêt.
- 2** Arrêtez les nœuds de Manager Service et attendez la fin de l'arrêt.
- 3** Dans les déploiements distribués avec plusieurs nœuds Web, arrêtez les nœuds Web secondaires et attendez la fin de l'arrêt.
- 4** Arrêtez le nœud Web principal et attendez la fin de l'arrêt.
- 5** Dans les déploiements distribués avec plusieurs dispositifs vRealize Automation en mode synchrone, utilisez l'interface de gestion du dispositif vRealize Automation pour passer en mode asynchrone.
- 6** Dans les déploiements distribués avec plusieurs dispositifs vRealize Automation, arrêtez les dispositifs secondaires et attendez la fin de l'arrêt.
- 7** Arrêtez le dispositif vRealize Automation principal et attendez la fin de l'arrêt.

Le dispositif vRealize Automation principal est celui qui contient la base de données de dispositif principal ou inscriptible. Notez quel dispositif est le dispositif principal pour que vous puissiez commencer à sauvegarder dans le bon ordre.

- 8** Dans n'importe quel ordre, arrêtez les serveurs MS SQL vRealize Automation autonomes et attendez la fin de l'arrêt.
- 9** Si vous utilisez une base de données PostgreSQL autonome héritée, arrêtez ce serveur.

Mise à jour de certificats vRealize Automation

Un administrateur système peut mettre à jour ou remplacer les certificats des composants vRealize Automation.

vRealize Automation contient trois composants principaux qui utilisent des certificats SSL pour assurer une communication sécurisée entre eux :

- Dispositif vRealize Automation
- Composant de site Web IaaS
- Composant de service de gestionnaire IaaS

En outre, votre déploiement peut disposer de certificats pour le site Web d'interface de gestion de dispositif vRealize Automation. Chaque machine IaaS exécute également un agent de gestion qui utilise un certificat.

Note vRealize Automation utilise plusieurs produits tiers, tels que Rabbit MQ, pour prendre en charge une grande variété de fonctionnalités. Certains de ces produits utilisent leurs propres certificats auto-signés qui sont conservés, même si vous remplacez les certificats vRealize Automation principaux par des certificats fournis par une autorité de certification. En raison de cette situation, les utilisateurs ne peuvent pas contrôler efficacement l'utilisation des certificats sur des ports spécifiques, par exemple le port 5671 qui est utilisé par RabbitMQ pour la communication interne.

À une exception près, les modifications apportées aux composants ultérieures de cette liste n'affectent pas les composants antérieurs. En revanche, un certificat mis à jour pour les composants IaaS doit être enregistré auprès du dispositif vRealize Automation.

Généralement, des certificats auto-signés sont générés et appliqués à ces composants pendant l'installation du produit. Vous pouvez remplacer un certificat pour passer de certificats auto-signés à des certificats fournis par une autorité de certification ou à l'expiration d'un certificat. Lorsque vous remplacez un certificat pour un composant vRealize Automation, les relations d'approbation pour d'autres composants vRealize Automation sont automatiquement mises à jour.

Par exemple, dans un système distribué comportant plusieurs instances de dispositif vRealize Automation, si vous mettez à jour un certificat pour une instance de dispositif vRealize Automation tous les autres certificats associés sont automatiquement mis à jour.

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.

L'interface de gestion du dispositif vRealize Automation fournit des options pour mettre à jour ou remplacer des certificats.

Dans un déploiement en cluster, vous devez initier les modifications à partir de l'interface du nœud principal.

- **Générer un certificat** : demandez à vRealize Automation de générer un certificat auto-signé.
- **Importer le certificat** : utilisez votre propre certificat.
- **Fournir l'empreinte numérique du certificat** : fournit une empreinte numérique de certificat pour utiliser un certificat déjà présent dans le magasin de certificats sur les serveurs Windows IaaS.

Cette option ne transmet pas le certificat du dispositif vRealize Automation aux serveurs Windows IaaS. L'option permet aux utilisateurs de déployer des certificats existants sur des serveurs Windows IaaS sans télécharger les certificats dans l'interface de gestion du dispositif vRealize Automation.

- **Conserver l'existant** : continuer à utiliser le certificat actuel.

Les certificats du site Web d'interface de gestion du dispositif vRealize Automation n'ont pas de conditions requises d'enregistrement.

Note Si votre certificat utilise une phrase secrète pour le chiffrement et que vous ne l'entrez pas lorsque vous remplacez votre certificat sur le dispositif, le remplacement du certificat échoue et le message `Unable to load private key` s'affiche.

Modèles de machine virtuelle

Après la modification des certificats du dispositif vRealize Automation ou du serveur Windows IaaS, vous devez mettre à jour les agents invités et logiciels de vRealize Automation sur les modèles de machine virtuelle afin que les modèles fonctionnent de nouveau dans vRealize Automation. Si vous ne mettez pas à jour les agents, les demandes de déploiement impliquant des composants logiciels échouent avec une erreur semblable à l'exemple suivant.

```
The following component requests failed: Linux. Request failed: Machine VM-001:
InstallSoftwareWorkflow. Install software work item timeout.
```

vRealize Orchestrator

Après la modification des certificats vRealize Automation, vous devez mettre à jour vRealize Orchestrator pour approuver les nouveaux certificats.

Le composant vRealize Orchestrator associé à votre déploiement vRealize Automation dispose de ses propres certificats, mais il doit également approuver les certificats vRealize Automation. Par défaut, le composant vRealize Orchestrator est intégré dans vRealize Automation, bien que quelques utilisateurs préfèrent utiliser une instance externe de vRealize Orchestrator. Dans les deux cas, consultez la documentation de vRealize Orchestrator pour plus d'informations sur la mise à jour des certificats vRealize Orchestrator.

Si vous exécutez un déploiement vRealize Orchestrator à nœuds multiples se trouvant derrière un équilibrage de charge, tous les nœuds vRealize Orchestrator doivent utiliser le même certificat.

Pour plus d'informations

Pour en savoir plus sur le dépannage des certificats, la capacité de prise en charge et les conditions d'approbation, consultez [l'article 2106583 de la base de connaissances VMware](#).

Extraction de certificats et de clés privées

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

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

Tableau 1-2. Modèle de valeurs de certificat et de commandes (openssl)

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

Remplacer des certificats dans le dispositif vRealize Automation

L'administrateur système peut mettre à jour ou remplacer un certificat autosigné par un certificat approuvé par une autorité de certification. Vous pouvez utiliser des certificats SAN (Subject Alternative Name), des certificats génériques ou toute autre méthode de certification réutilisable adaptée à votre environnement, tant que vous respectez les conditions requises en matière d'approbation.

Lorsque vous mettez à jour ou remplacez le certificat du dispositif vRealize Automation, l'approbation d'autres composants associés est initiée à nouveau automatiquement. Pour plus d'informations sur la mise à jour des certificats, reportez-vous à la section [Mise à jour de certificats 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 **vRA > Certificats**.
- 3 Sélectionnez le composant vRealize Automation pour lequel vous mettez à jour le certificat.

4 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 | <ol style="list-style-type: none"> a La valeur affichée dans la zone de texte Nom commun est celle du nom d'hôte, tel qu'il s'affiche dans la partie supérieure de la page. Si des instances supplémentaires du dispositif vRealize Automation 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. |

5 Cliquez sur **Enregistrer les paramètres**.

Une mise à jour du certificat du dispositif vRealize Automation requiert que les services vRealize Automation redémarrent normalement. Le redémarrage peut prendre de 15 minutes à une heure selon le nombre de dispositifs vRealize Automation dans votre environnement.

Après le redémarrage, les détails du certificat de toutes les instances applicables du dispositif vRealize Automation s'affichent sur la page.

6 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 la console de gestion du dispositif vRealize Automation en tant qu'utilisateur racine.
- b Cliquez sur l'onglet **Admin**.
- c Cliquez sur le sous-menu **Admin**.
- d Sélectionnez la case **Service SSH activé**.

Désélectionnez la case pour désactiver SSH une fois terminé.

- e Sélectionnez la case **Connexion SSH de l'administrateur**.
Désélectionnez la case pour désactiver SSH une fois terminé.
 - f Cliquez sur **Enregistrer les paramètres**.
- 7** Vérifiez que vous pouvez vous connecter à la console vRealize Automation.
- a Ouvrez un navigateur et accédez à `https://vcac-hostname.domain.name/vcac`.
Si vous utilisez un équilibrage de charge, le nom d'hôte doit être le nom de domaine complet de l'équilibrage de charge.
 - b Si vous y êtes invité, poursuivez après les avertissements de certificat.
 - c Connectez-vous avec l'identifiant **administrator@vsphere.local** et le mot de passe que vous avez spécifié lorsque vous avez configuré la Gestion des annuaires.
La console s'ouvre sur la page **Locataires** dans l'onglet **Administration**. Un locataire nommé `vsphere.local` figure dans la liste.
- 8** Si vous utilisez un équilibrage de charge, configurez et activez tous les contrôles de santé applicables.

Résultats

Le certificat est mis à jour.

Remplacer le certificat d'Infrastructure en tant que service

L'administrateur système peut remplacer un certificat expiré ou un certificat autosigné par celui d'une autorité de certification pour garantir la sécurité d'un environnement de déploiement distribué.

Vous pouvez utiliser un certificat SAN sur plusieurs machines. Les certificats utilisés pour les composants IaaS (site Web et Manager Service) doivent être émis avec des valeurs SAN, notamment les noms de domaine complets de tous les hôtes Windows sur lesquels le composant correspondant est installé, et avec le nom de domaine complet de l'équilibrage de charge du même composant.

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 > Certificats**.
- 3** Cliquez sur **IaaS Web** dans le menu **Type de composant**.
- 4** Accédez au volet **Certificat Web IaaS**.

5 Sélectionnez l'option de remplacement de certificat dans le menu **Action de certificat**.

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

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

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 | Description |
|--|--|
| Conserver l'existant | Conserver la configuration SSL actuelle. Sélectionnez cette option pour annuler vos modifications. |
| Générer un certificat | <ol style="list-style-type: none"> a La valeur affichée dans la zone de texte Nom commun est celle du nom d'hôte, tel qu'il s'affiche dans la partie supérieure de la page. Si des instances supplémentaires du dispositif vRealize Automation sont disponibles, leurs noms de domaine complets sont inclus dans l'attribut SAN du certificat. b Entrez le nom de votre organisation, comme le nom de votre société, dans la zone de texte Organisation. c Entrez votre unité d'organisation, comme le nom ou l'emplacement de votre service, dans la zone de texte Unité d'organisation. d Entrez un code pays ISO 3166, comme FR, dans la zone de texte Pays. |
| Importer | <ol style="list-style-type: none"> a Copiez les valeurs du certificat de BEGIN PRIVATE KEY à END PRIVATE KEY, en incluant l'en-tête et le pied de page, et collez-les dans la zone de texte Clé privée RSA. b Copiez les valeurs du certificat de BEGIN CERTIFICATE à END CERTIFICATE, en incluant l'en-tête et le pied de page, dans la zone de texte Chaîne de certificat. Pour les valeurs de certificats multiples, incluez un en-tête BEGIN CERTIFICATE et un pied de page END CERTIFICATE pour chaque certificat. <p>Note Dans le cas de certificats en chaînes, des attributs supplémentaires peuvent être disponibles.</p> <ol 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. |
| Fournir l'empreinte numérique du certificat | Utilisez cette option si vous souhaitez fournir une empreinte numérique du certificat afin d'utiliser un certificat déjà déployé dans le magasin de certificats des serveurs IaaS. L'utilisation de cette option ne transmet pas le certificat du dispositif virtuel aux serveurs IaaS. Elle permet aux utilisateurs de déployer des certificats existants sur des serveurs IaaS sans les télécharger dans l'interface de gestion. |

6 Cliquez sur **Enregistrer les paramètres**.

Une mise à jour du certificat du serveur Windows IaaS requiert que les services vRealize Automation redémarrent normalement. Le redémarrage peut prendre de 15 minutes à une heure selon le nombre de dispositifs vRealize Automation dans votre environnement.

Après le redémarrage, les détails du certificat s'affichent sur la page.

Remplacer le certificat IaaS Manager Service

Un administrateur système peut remplacer un certificat expiré ou un certificat autosigné par celui d'une autorité de certification pour garantir la sécurité d'un environnement de déploiement distribué.

Vous pouvez utiliser un certificat SAN sur plusieurs machines. Les certificats utilisés pour les composants IaaS (site Web et Manager Service) doivent être émis avec des valeurs SAN, notamment les noms de domaine complets de tous les hôtes Windows sur lesquels le composant correspondant est installé, et avec le nom de domaine complet de l'équilibrage de charge du même composant.

IaaS Manager Service et IaaS Web Service partagent un certificat unique.

Procédure

- 1 Ouvrez un navigateur Web et accédez à l'URL de l'interface de gestion du dispositif vRealize Automation.
- 2 Connectez-vous avec le nom d'utilisateur **root** et le mot de passe que vous avez spécifiés lors du déploiement du dispositif vRealize Automation.
- 3 Sélectionnez **vRA > Certificats**.
- 4 Cliquez sur **Manager Service** dans le menu **Type de composant**.
- 5 Sélectionnez le type de certificat dans le menu **Action de certificat**.

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

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

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 | Description |
|--|--|
| 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. |
| 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. <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. |
| Fournir l'empreinte numérique du certificat | Utilisez cette option si vous souhaitez fournir une empreinte numérique du certificat afin d'utiliser un certificat déjà déployé dans le magasin de certificats des serveurs IaaS. L'utilisation de cette option ne transmet pas le certificat du dispositif virtuel aux serveurs IaaS. Elle permet aux utilisateurs de déployer des certificats existants sur des serveurs IaaS sans les télécharger dans l'interface de gestion. |

6 Cliquez sur **Enregistrer les paramètres**.

Quelques minutes plus tard, les détails du certificat s'affichent sur la page.

7 Si votre réseau ou votre équilibrage de charge l'exige, copiez dans l'équilibrage de charge le certificat importé ou récemment créé.

- 8 Ouvrez un navigateur et accédez à l'adresse `https://managerServiceAddress/vmpsProvision/` depuis un serveur qui exécute un DEM Worker ou un agent.

Si vous utilisez un équilibrage de charge, le nom d'hôte doit être le nom de domaine complet de l'équilibrage de charge.

- 9 Si vous y êtes invité, poursuivez après les avertissements de certificat.
- 10 Confirmez que le nouveau certificat est fourni et approuvé.
- 11 Si vous utilisez un équilibrage de charge, configurez et activez tous les contrôles de santé applicables.

Mettre à jour une instance intégrée de vRealize Orchestrator pour lui permettre d'approuver les certificats vRealize Automation

Si vous mettez à jour ou modifiez les certificats dispositif vRealize Automation ou IaaS, vous devez mettre à jour vRealize Orchestrator pour qu'il approuve les nouveaux certificats ou ceux mis à jour.

Cette procédure s'applique à tous les déploiements vRealize Automation qui utilisent une instance intégrée de vRealize Orchestrator. Si vous utilisez une instance externe de vRealize Orchestrator, reportez-vous à la section [Mettre à jour l'instance externe de vRealize Orchestrator pour qu'elle approuve les certificats vRealize Automation](#).

Note Cette procédure rétablit les paramètres par défaut de l'authentification de locataire et de groupe. Si vous avez personnalisé la configuration de l'authentification, notez vos modifications afin que vous puissiez reconfigurer l'authentification après avoir terminé la procédure.

Consultez la documentation de vRealize Orchestrator pour plus d'informations sur la mise à jour et le remplacement des certificats vRealize Orchestrator.

Dans une configuration en cluster, vous devez effectuer cette procédure sur le nœud principal du dispositif vRealize Automation, puis exécuter l'opération `join-cluster` sur le nœud principal à partir de chaque nœud de dispositif vRealize Automation de réplica.

Note Dans un cluster, arrêtez le service `vco-configurator` sur tous les nœuds de réplica jusqu'à ce que la procédure soit terminée pour éviter une synchronisation automatique indésirable du centre de contrôle.

Si vous remplacez ou mettez à jour des certificats vRealize Automation sans exécuter cette procédure, le centre de contrôle vRealize Orchestrator peut être inaccessible et des erreurs peuvent apparaître dans les fichiers journaux `vco-server` et `vco-configurator`.

Des problèmes de mise à jour des certificats peuvent également survenir si vRealize Orchestrator est configuré pour vous authentifier auprès d'un locataire et un groupe autre que vRealize Automation. Pour plus d'informations, reportez-vous à l'article [Exception : chaîne de certificats non approuvés après le remplacement du certificat vRA \(2147612\)](#) de la base de connaissances VMware.

Les syntaxes des commandes d'approbation présentées ici sont représentatives et non définitives. Bien qu'elles soient adaptées à la plupart des déploiements courants, dans certaines situations vous devrez essayer des variantes de ces commandes.

- Si vous spécifiez `--certificate`, vous devez fournir le chemin d'accès à un fichier de certificat valide au format PEM.
- Si vous spécifiez `--uri`, vous devez fournir l'URI à partir duquel la commande peut extraire un certificat approuvé.
- Si vous spécifiez l'option `--registry-certificate`, vous indiquez que le certificat demandé doit être traité comme le certificat pour le registre de composants et que le certificat approuvé est ajouté au magasin d'approbations sous un alias spécifique utilisé par le certificat de registre du composant.

Vous pouvez également gérer les certificats à l'aide des workflows Gestionnaire de confiance SSL dans vRealize Orchestrator. Pour plus d'informations, consultez la section *Gérer les certificats Orchestrator* dans la [documentation de vRealize Orchestrator](#).

Procédure

- 1 Arrêtez le serveur vRealize Orchestrator et les services de centre de contrôle.

```
service vco-server stop
service vco-configurator stop
```

- 2 Réinitialisez le fournisseur d'authentification vRealize Orchestrator en exécutant la commande suivante.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh reset-authentication
ls -l /etc/vco/app-server/
mv /etc/vco/app-server/vco-registration-id /etc/vco/app-server/vco-registration-id.old
vcac-vami vco-service-reconfigure
```

- 3 Vérifiez le certificat approuvé pour le magasin d'approbations vRealize Orchestrator à l'aide de l'utilitaire de l'interface de ligne de commande situé dans `/var/lib/vco/tools/configuration-cli/bin` avec la commande suivante.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh list-trust
```

- Vérifiez le certificat ayant l'alias suivant : `vco.cafe.component-registry.ssl.certificate`. Ce devrait être le certificat vRealize Automation que l'instance de vRealize Orchestrator utilise comme fournisseur d'authentification.
- Ce certificat doit correspondre au certificat de vRealize Automation récemment configuré. S'il ne correspond pas, pour en changer, procédez comme suit :
 - 1 Copiez votre fichier PEM de certificat de dispositif signé vRealize Automation dans le dossier `/tmp` sur le dispositif.

- 2 Exécutez la commande suivante ajoutant le chemin d'accès approprié au certificat.

```
./vro-configure.sh trust --certificate path-to-the-certificate-file-in-PEM-format--registry-certificate
```

Voir l'exemple de commande suivant :

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh trust --certificate /var/tmp/test.pem --registry-certificate
```

- 4 Vous devrez éventuellement exécuter les commandes suivantes pour approuver le certificat.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh trust --uri https://vra.domain.com  
  
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh trust --registry-certificate --uri https://vra.domain.com
```

- 5 Assurez-vous que le certificat vRealize Automation est maintenant injecté dans le magasin d'approbations vRealize Orchestrator à l'aide de la commande suivante.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh list-trust
```

- 6 Démarrez le serveur vRealize Orchestrator et les services du centre de contrôle.

```
service vco-server start  
service vco-configurator start
```

Étape suivante

Vous pouvez confirmer que l'approbation a été mise à jour sur un système en cluster.

- 1 Connectez-vous à l'interface de gestion de dispositifs virtuels en tant qu'utilisateur racine.

- 2 Sélectionnez la page Services.

- 3 Assurez-vous qu'aucun service vco en double n'est répertorié.

Si vous voyez une duplication des services vco répertoriée, cliquez sur **Annuler l'enregistrement** pour supprimer les services qui n'ont pas l'état Registered.

- 4 Assurez-vous que vco-configurator est démarré sur tous les nœuds de dispositifs virtuels.

- 5 Connectez-vous au centre de contrôle vRealize Orchestrator et accédez à la page Valider la configuration pour valider la configuration.

- 6 Accédez à la page Fournisseur d'authentification et vérifiez que les paramètres d'authentification sont corrects.

Vous pouvez également tester les informations d'identification de connexion sur cette page.

Mettre à jour l'instance externe de vRealize Orchestrator pour qu'elle approuve les certificats vRealize Automation

Si vous mettez à jour ou modifiez les certificats dispositif vRealize Automation ou IaaS, vous devez mettre à jour vRealize Orchestrator pour qu'il approuve les nouveaux certificats ou ceux mis à jour.

Cette procédure s'applique aux déploiements vRealize Automation qui utilisent une instance externe de vRealize Orchestrator.

Note Cette procédure rétablit les paramètres par défaut de l'authentification de locataire et de groupe. Si vous avez personnalisé la configuration de l'authentification, notez vos modifications afin que vous puissiez reconfigurer l'authentification après avoir terminé la procédure.

Consultez la documentation de vRealize Orchestrator pour plus d'informations sur la mise à jour et le remplacement des certificats vRealize Orchestrator.

Si vous remplacez ou mettez à jour des certificats vRealize Automation sans exécuter cette procédure, le centre de contrôle vRealize Orchestrator peut être inaccessible et des erreurs peuvent apparaître dans les fichiers journaux vco-server et vco-configurator.

Des problèmes de mise à jour des certificats peuvent également survenir si vRealize Orchestrator est configuré pour vous authentifier auprès d'un locataire et un groupe autre que vRealize Automation. Consultez l'[article 2147612 de la Base de connaissances](#).

Procédure

- 1 Arrêtez le serveur vRealize Orchestrator et les services de centre de contrôle.

```
service vco-configurator stop
```

- 2 Réinitialisez le fournisseur d'authentification vRealize Orchestrator.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh reset-authentication
```

- 3 Démarrez le service de centre de contrôle vRealize Orchestrator.

```
service vco-configurator start
```

- 4 Connectez-vous au centre de contrôle en utilisant les informations d'identification de l'utilisateur racine de l'interface de gestion de dispositif virtuel.

- 5 Annulez l'enregistrement du fournisseur d'authentification et réenregistrez-le.

Mise à jour du certificat du site de gestion de dispositifs vRealize Automation

L'administrateur système peut remplacer le certificat SSL du service de site de gestion lorsque celui-ci expire ou remplacer un certificat autosigné par un certificat émis par une autorité de certification. Vous sécurisez le service de site de gestion sur le port 5480.

Le dispositif vRealize Automation utilise lighttpd pour exécuter son propre site de gestion. Lorsque vous remplacez un certificat de site de gestion, vous devez également configurer tous les agents de gestion pour qu'ils reconnaissent le nouveau certificat.

Si vous exécutez un déploiement distribué, vous pouvez mettre à jour les agents de gestion automatiquement ou manuellement. Si vous exécutez un déploiement minimal, vous devez mettre à jour l'agent de gestion manuellement.

Consultez [Mettre à jour manuellement la reconnaissance de certificat d'agent de gestion](#) pour plus d'informations.

Procédure

1 Rechercher l'identifiant d'agent de gestion

Vous utilisez l'identifiant d'agent de gestion lorsque vous créez et inscrivez un nouveau certificat de serveur de site de gestion.

2 Remplacer le certificat du site de gestion des dispositifs vRealize Automation

Si le certificat SSL du service du site de gestion expire ou si vous avez démarré avec un certificat auto-signé et que les stratégies de site en nécessitent un autre, vous pouvez remplacer le certificat.

3 Mettre à jour la reconnaissance du certificat de l'agent de gestion

Après avoir remplacé un certificat de site de gestion de dispositif vRealize Automation, vous devez mettre à jour tous les agents de gestion pour qu'ils reconnaissent le nouveau certificat afin de rétablir des communications approuvées entre le site de gestion des dispositifs virtuels et les agents de gestion des hôtes IaaS.

Rechercher l'identifiant d'agent de gestion

Vous utilisez l'identifiant d'agent de gestion lorsque vous créez et inscrivez un nouveau certificat de serveur de site de gestion.

Procédure

- 1 Ouvrez le fichier de configuration de l'agent de gestion situé à `<vra-installation-dir>\Management Agent\VMware.IaaS.Management.Agent.exe.config`.

- 2 Enregistrez la valeur à partir de l'attribut id de l'élément agentConfiguration.

```
<agentConfiguration id="0E22046B-9D71-4A2B-BB5D-70817F901B27">
```

Remplacer le certificat du site de gestion des dispositifs vRealize Automation

Si le certificat SSL du service du site de gestion expire ou si vous avez démarré avec un certificat auto-signé et que les stratégies de site en nécessitent un autre, vous pouvez remplacer le certificat.

Vous êtes autorisé à réutiliser le certificat utilisé par le service vRealize Automation sur le port 443 ou d'en utiliser un autre. Si vous demandez un nouveau certificat émis par l'autorité de certification pour mettre à jour un certificat existant, il est recommandé de réutiliser le nom commun à partir du certificat existant.

Note Le dispositif vRealize Automation utilise lighttpd pour exécuter son propre site de gestion. Vous sécurisez le service de site de gestion sur le port 5480.

Conditions préalables

- Le certificat doit être au format PEM.
- Le certificat doit inclure les deux éléments suivants, dans l'ordre, ensemble dans un seul fichier :
 - a Clé privée RSA
 - b Chaîne de certificats
- La clé privée ne peut pas être chiffrée.
- L'emplacement et le nom de fichier par défaut est `/opt/vmware/etc/lighttpd/server.pem`.

Pour obtenir des informations sur l'exportation d'un certificat et d'une clé privée d'un magasin de clés Java vers un fichier PEM, consultez [Extraction de certificats et de clés privées](#).

Procédure

- 1 Connectez-vous à l'aide de la console du dispositif ou SSH.
- 2 Sauvegardez votre fichier de certificat actuel.

```
cp /opt/vmware/etc/lighttpd/server.pem /opt/vmware/etc/lighttpd/server.pem-bak
```

- 3 Copiez le nouveau certificat sur votre dispositif en remplaçant le contenu du fichier `/opt/vmware/etc/lighttpd/server.pem` par les informations sur le nouveau certificat.
- 4 Pour redémarrer le serveur lighttpd, exécutez la commande suivante :

```
service vami-lighttp restart
```
- 5 Exécutez la commande suivante pour redémarrer le service HAProxy :

```
service haproxy restart
```
- 6 Connectez-vous à la console de gestion et confirmez le remplacement du certificat. Vous pouvez avoir besoin de redémarrer votre navigateur.

Étape suivante

Mettez à jour tous les agents de gestion pour reconnaître le nouveau certificat.

Pour les déploiements distribués, vous pouvez mettre à jour les agents de gestion manuellement ou automatiquement. Pour les installations minimales, vous devez procéder manuellement à la mise à jour des agents.

- Pour plus d'informations sur la mise à jour automatique, reportez-vous à la section [Mettre à jour automatiquement des agents de gestion dans un environnement distribué pour reconnaître un certificat de site de gestion des dispositifs vRealize Automation](#).
- Pour plus d'informations sur la mise à jour manuelle, reportez-vous à la section [Mettre à jour manuellement la reconnaissance de certificat d'agent de gestion](#).

Mettre à jour la reconnaissance du certificat de l'agent de gestion

Après avoir remplacé un certificat de site de gestion de dispositif vRealize Automation, vous devez mettre à jour tous les agents de gestion pour qu'ils reconnaissent le nouveau certificat afin de rétablir des communications approuvées entre le site de gestion des dispositifs virtuels et les agents de gestion des hôtes IaaS.

Chaque hôte IaaS exécute un agent de gestion et chaque agent de gestion doit être mis à jour. Les déploiements minimaux doivent être mis à jour manuellement, tandis que les déploiements distribués peuvent être mis à jour manuellement ou à l'aide d'un processus automatisé.

- [Mettre à jour manuellement la reconnaissance de certificat d'agent de gestion](#)
Après avoir remplacé un certificat de site de gestion de dispositif vRealize Automation, vous devez mettre à jour manuellement les agents de gestion pour qu'ils reconnaissent le nouveau certificat afin de rétablir des communications approuvées entre le site de gestion des dispositifs virtuels et les agents de gestion des hôtes IaaS.
- [Mettre à jour automatiquement des agents de gestion dans un environnement distribué pour reconnaître un certificat de site de gestion des dispositifs vRealize Automation](#)
Après la mise à jour du certificat du site de gestion dans un déploiement haute disponibilité, la configuration de l'agent de gestion doit également être mise à jour pour reconnaître le nouveau certificat et rétablir une communication approuvée.

Mettre à jour manuellement la reconnaissance de certificat d'agent de gestion

Après avoir remplacé un certificat de site de gestion de dispositif vRealize Automation, vous devez mettre à jour manuellement les agents de gestion pour qu'ils reconnaissent le nouveau certificat afin de rétablir des communications approuvées entre le site de gestion des dispositifs virtuels et les agents de gestion des hôtes IaaS.

Procédez comme suit pour chaque agent de gestion de votre déploiement après avoir remplacé un certificat du site de gestion du dispositif vRealize Automation.

Pour les déploiements distribués, vous pouvez mettre à jour les agents de gestion manuellement ou automatiquement. Pour plus d'informations sur la mise à jour automatique, reportez-vous à la section [Mettre à jour automatiquement des agents de gestion dans un environnement distribué pour reconnaître un certificat de site de gestion des dispositifs vRealize Automation](#).

Conditions préalables

Enregistrez les empreintes SHA1 du nouveau certificat de site de gestion de dispositif vRealize Automation.

Procédure

- 1 Arrêtez le service de l'agent de gestion VMware vCloud Automation Center.
- 2 Accédez au fichier de configuration de l'agent de gestion situé à l'adresse `[vcac_installation_folder]\Management Agent\VMware.IaaS.Management.Agent.exe.Config`, en général `C:\Program Files (x86)\VMware\VCAC\Management Agent\VMware.IaaS.Management.Agent.exe.Config`.
- 3 Ouvrez le fichier pour le modifier et recherchez le paramètre de configuration du point de terminaison de l'ancien certificat de site de gestion, que vous pouvez identifier à l'aide de l'adresse de point de terminaison.

Par exemple :

```
<agentConfiguration id="C816CFBC-4830-4FD2-8951-C17429CEA291" pollingInterval="00:03:00">
  <managementEndpoints>
    <endpoint address="https://vra-va.local:5480"
thumbprint="D1542471C30A9CE694A512C5F0F19E45E6FA32E6" />
  </managementEndpoints>
</agentConfiguration>
```

- 4 Modifiez l'empreinte avec l'empreinte SHA1 du nouveau certificat.

Par exemple :

```
<agentConfiguration id="C816CFBC-4830-4FD2-8951-C17429CEA291" pollingInterval="00:03:00">
  <managementEndpoints>
    <endpoint address="https://vra-va.local:5480"
thumbprint="8598B073359BAE7597F04D988AD2F083259F1201" />
  </managementEndpoints>
</agentConfiguration>
```

- 5 Démarrez le service de l'agent de gestion VMware vCloud Automation Center.
- 6 Connectez-vous au site de gestion de dispositif virtuel et sélectionnez l'onglet **Cluster**.
- 7 Consultez le tableau Informations sur le déploiement distribué pour vérifier que le serveur IaaS a contacté le dispositif virtuel récemment, ce qui confirme que la mise à jour a réussi.

Mettre à jour automatiquement des agents de gestion dans un environnement distribué pour reconnaître un certificat de site de gestion des dispositifs vRealize Automation

Après la mise à jour du certificat du site de gestion dans un déploiement haute disponibilité, la configuration de l'agent de gestion doit également être mise à jour pour reconnaître le nouveau certificat et rétablir une communication approuvée.

Vous pouvez mettre à jour les informations du certificat du site de gestion du dispositif vRealize Automation pour les systèmes distribués manuellement ou automatiquement. Pour plus d'informations sur la mise à niveau manuelle des agents de gestion, reportez-vous à la section [Mettre à jour manuellement la reconnaissance de certificat d'agent de gestion](#).

Utilisez cette procédure pour mettre à jour automatiquement les informations du certificat.

Procédure

- 1 Lorsque des agents de gestion sont en cours d'exécution, remplacez le certificat sur un site unique de gestion du dispositif vRealize Automation de votre déploiement.
- 2 Attendez quinze minutes que l'agent de gestion se synchronise avec le nouveau certificat du site de gestion du dispositif vRealize Automation.
- 3 Remplacez les certificats sur les autres sites de gestion du dispositif vRealize Automation de votre déploiement.

Les agents de gestion sont automatiquement mis à jour avec les informations du nouveau certificat.

Remplacer un certificat d'agent de gestion

L'administrateur système peut remplacer le certificat d'agent de gestion lorsque celui-ci expire ou remplacer un certificat autosigné par un certificat émis par une autorité de certification.

Chaque hôte IaaS exécute son propre agent de gestion. Répétez cette procédure sur chaque nœud IaaS dont vous souhaitez mettre à jour l'agent de gestion.

Conditions préalables

- Copiez l'identifiant de l'agent de gestion dans la colonne ID du nœud avant de supprimer l'enregistrement. Cet identifiant vous est utile lors de la création du nouveau certificat de l'agent de gestion et de son enregistrement.
- Lorsque vous demandez un nouveau certificat, assurez-vous que le format du champ Nom commun figurant dans l'objet du nouveau certificat est le suivant :

```
VMware Management Agent 00000000-0000-0000-0000-000000000000
```

Utilisez la chaîne VMware Management Agent, suivie d'un seul espace et du GUID de l'agent de gestion au format numérique indiqué.

Procédure

- 1 Arrêtez le service Agent de gestion de votre composant logiciel enfichable Services Windows.
 - a Sur votre machine Windows, cliquez sur **Démarrer**.
 - b Dans la zone Rechercher de Windows, entrez **services.msc** et appuyez sur Entrée.
 - c Cliquez avec le bouton droit sur le service **Agent de gestion de VMware vCloud Automation Center** et cliquez sur **Arrêter** pour arrêter le service.
- 2 Supprimez le certificat actuel de la machine. Pour plus d'informations sur la gestion des certificats sur Windows Server 2008 R2, reportez-vous à l'article de la Base de connaissances Microsoft à l'adresse <http://technet.microsoft.com/en-us/library/cc772354.aspx> ou à l'article wiki de Microsoft à l'adresse <http://social.technet.microsoft.com/wiki/contents/articles/2167.how-to-use-the-certificates-console.aspx>.
 - a Ouvrez la console de gestion Microsoft à l'aide de la commande **mmc.exe**.
 - b Appuyez sur Ctrl + M pour ajouter un nouveau fichier enfichable à la console ou choisissez l'option dans le menu déroulant Fichier.
 - c Sélectionnez **Certificats** et cliquez sur **Ajouter**.
 - d Sélectionnez **Compte ordinateur** et cliquez sur **Suivant**.
 - e Sélectionnez **Ordinateur local : (ordinateur sur lequel cette console s'exécute)**.
 - f Cliquez sur **OK**.
 - g Développez la zone **Certificats (Ordinateur local)** sur le côté gauche de la console.
 - h Développez la zone **Personnel** et sélectionnez le dossier Certificats.
 - i Sélectionnez le certificat d'agent de gestion actuel et cliquez sur **Supprimer**.
 - j Cliquez sur **Oui** pour confirmer la suppression.
- 3 Importez le certificat venant d'être généré dans le magasin `computer.personal` local ou n'importez rien si vous voulez que le système génère automatiquement un nouveau certificat auto-signé.

4 Enregistrez le certificat de l'agent de gestion sur le site de gestion du dispositif vRealize Automation.

- a Ouvrez une invite de commande en tant qu'administrateur et accédez au répertoire `Cafe` de la machine sur lequel l'agent de gestion est installé à l'emplacement `<vra-installation-dir>\Management Agent\Tools\Cafe`, en général `C:\Program Files (x86)\VMware\VCAC\Management Agent\Tools\Cafe`.
- b Entrez la commande `Vcac-Config.exe RegisterNode` avec les options permettant d'enregistrer l'identifiant et le certificat de l'agent de gestion en une seule étape. Incluez l'identifiant d'agent de gestion enregistré auparavant comme valeur pour l'option `-nd`.

Tableau 1-3. Options et arguments requis pour la commande Vcac-Config.exe
RegisterNode

[illegible]

L'exemple suivant indique le format de la commande :

```
Vcac-Config.exe RegisterNode -v -vamih "vra-vr-hostname.domain.name:5480"  
-cu "root" -cp "password" -hn "machine-hostname.domain.name"  
-nd "00000000-0000-0000-0000-000000000000"  
-tp "00000000000000000000000000000000000000000000"
```

- 5** Redémarrez l'Agent de gestion.

Exemple : Commande permettant d'enregistrer un certificat d'agent de gestion

```
Vcac-Config.exe RegisterNode -v -vamih "vra-va.eng.mycompany:5480" -cu "root" -cp
"secret" -hn "iaas.eng.mycompany" -nd "C816CFBX-4830-4FD2-8951-C17429CEA291" -tp
"70928851D5B72B206E4B1CF9F6ED953EE1103DED"
```

Modifier la méthode d'interrogation pour des certificats

En présence de virgules dans la section OU du certificat IaaS, vous pouvez rencontrer des erreurs STOMP WebSocket dans les fichiers journaux de Manager Service. En outre, le provisionnement de la machine virtuelle peut échouer. Vous pouvez supprimer les virgules ou remplacer la méthode d'interrogation WebSocket par HTTP.

Pour modifier la méthode d'interrogation, procédez comme suit.

Procédure

- 1** Ouvrez le fichier suivant dans un éditeur de texte.

C:\\Program Files (x86)\\VMware\\vCAC\\Server\\Manager Service.exe.config.

- 2** Ajoutez les lignes 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"/>
```

- 3** Enregistrez et fermez Manager Service.exe.config.

- #### 4 Redémarrez Manager Service.

Résultats

Pour plus d'informations sur Manager Service, consultez *Installation de vRealize Automation*.

Gestion de la base de données de dispositif Postgres vRealize Automation

vRealize Automation requiert la base de données du dispositif pour les opérations système. Vous pouvez gérer la base de données du dispositif au moyen de l'interface VAMI (Virtual Appliance Management Interface) de vRealize Automation.

Note Ces informations s'appliquent uniquement aux déploiements qui utilisent une base de données de dispositif intégrée. Elles ne s'appliquent pas aux déploiements qui utilisent une base de données Postgres externe.

Vous pouvez configurer la base de données en tant que système à nœud unique ou à plusieurs nœuds pour faciliter la haute disponibilité au moyen du basculement. Le programme d'installation vRealize Automation inclut un nœud de base de données sur chaque installation du dispositif vRealize Automation. Si vous installez trois instances d'un dispositif vRealize Automation, vous disposez donc de trois nœuds de base de données. Le basculement automatique est implémenté sur les déploiements applicables. La base de données du dispositif ne nécessite aucun maintenance, sauf si une configuration de la machine change ou, si vous utilisez une configuration en cluster, vous promouvez un autre nœud comme principal.

Note La configuration en cluster de la base de données est définie automatiquement lorsque vous ajoutez un dispositif virtuel au cluster à l'aide de l'opération Joindre un cluster. Le cluster de base de données n'est pas directement dépendant du cluster du dispositif virtuel. Par exemple, une machine virtuelle jointe à un cluster peut fonctionner normalement même si la base de données du dispositif intégrée n'a pas démarré ou a échoué.

Pour la haute disponibilité, vRealize Automation utilise le modèle de réplica/principal PostgreSQL pour prendre en charge la réplication des données. Cela signifie que tous les nœuds de base de données fonctionnent dans un cluster avec un nœud de début, appelé principal, et plusieurs nœuds de réplication, appelés réplicas. Le nœud principal gère toutes les demandes de base de données et les nœuds de réplica diffusent et exécutent les transactions à partir du nœud principal localement.

Une configuration en cluster contient un nœud principal et un ou plusieurs nœuds de réplica. Le nœud principal est le nœud du dispositif vRealize Automation incluant la base de données principale qui prend en charge la fonctionnalité du système. Les nœuds de réplica contiennent des copies de la base de données qui peuvent être extraites en service en cas de panne du nœud principal.

Il existe plusieurs options de base de données de dispositif haute disponibilité. Le choix du mode de réplication est l'option de configuration de base de données la plus importante. Le mode de réplication détermine comment votre déploiement vRealize Automation maintient l'intégrité des données et, pour les configurations à haute disponibilité, comment il bascule en cas d'échec du nœud principal. Deux modes de réplication sont disponibles : synchrone et asynchrone.

Les deux modes prennent en charge le basculement de base de données, mais chacun possède des avantages et des inconvénients. Notez que pour prendre en charge le basculement vers la base de données à haute disponibilité, le mode asynchrone nécessite deux nœuds, tandis que le mode synchrone en nécessite trois. Le mode synchrone appelle également le basculement automatique.

| Mode de réplication | Avantages | Inconvénients |
|---------------------|---|--|
| Synchrone | <ul style="list-style-type: none"> ■ Minimise les risques de perte de données. ■ Appelle le basculement automatique. | <ul style="list-style-type: none"> ■ Peut affecter les performances du système. ■ Nécessite trois nœuds. |
| Asynchrone | <ul style="list-style-type: none"> ■ Nécessite seulement deux nœuds. ■ Affecte moins les performances du système que le mode synchrone. | Pas aussi efficace que le mode synchrone pour éviter la perte de données. |

vRealize Automation prend en charge les deux modes, mais fonctionne en mode asynchrone par défaut et offre une haute disponibilité uniquement s'il y a au moins deux nœuds de base de données de dispositif. L'onglet **Cluster** de l'interface VAMI (Virtual Appliance Management Interface) vous permet de changer de mode de synchronisation et d'ajouter des nœuds de base de données si nécessaire.

Lors de l'utilisation en mode synchrone, vRealize Automation appelle le basculement automatique.

si vous commencez avec un nœud dans une configuration qui n'est pas à haute disponibilité, vous pouvez ajouter des nœuds ultérieurement en fonction des besoins pour améliorer la haute disponibilité. Si vous possédez le matériel approprié et le niveau de protection maximum contre la perte de données, considérez la possibilité de configurer votre déploiement pour opérer en mode synchrone.

Basculement de la base de données du dispositif

Dans une configuration haute disponibilité, le server principal diffuse en permanence les transactions vers les serveurs répliqués. Si le serveur principal tombe en panne, le réplica actif et opérationnel est prêt à traiter des demandes en lecture seule. Lorsque le nouveau serveur principal est promu, manuellement ou automatiquement, toutes les demandes à venir y sont déplacées.

Configurer la base de données du dispositif

Vous pouvez utiliser la page de la base de données VAMI (Virtual Appliance Management Interface) pour contrôler ou mettre à jour la configuration de la base de données du dispositif. Vous pouvez également l'utiliser pour modifier la désignation du nœud principal et le mode de synchronisation utilisé par la base de données.

La base de données de dispositif est installée et configurée lors de l'installation et de la configuration du système vRealize Automation, mais vous pouvez contrôler et modifier la configuration depuis l'onglet **Administration** de la l'interface VAMI.

La zone de texte **État de connexion** indique si la base de données est connectée au système vRealize Automation et si elle fonctionne correctement.

Si votre base de données de dispositif utilise plusieurs nœuds pour prendre en charge le basculement, le tableau au bas de la page affiche les nœuds, ainsi que leur état et indique quel nœud est l'instance principale de. La zone de texte **Mode de réplication** indique le mode de fonctionnement configuré pour le système : synchrone ou asynchrone. Utilisez cette page pour mettre à jour la configuration de la base de données du dispositif.

La colonne État de synchronisation* du tableau de nœuds de la base de données indique la méthode de synchronisation pour le cluster. Associée à la colonne État, celle-ci indique l'état des nœuds de cluster. L'état peut varier selon que le cluster utilise la réplication synchrone ou asynchrone.

Tableau 1-4. État de synchronisation pour les modes de réplication de base de données de dispositif

| Mode | Message d'état de synchronisation |
|------------------------|--|
| Réplication synchrone | Nœud principal - aucun état Nœud de réplica - synchronisation Autres nœuds - potentiel |
| Réplication asynchrone | Nœud principal - aucun état Autres nœuds - potentiel |

La colonne valide indique si les réplicas sont synchronisés avec le nœud principal. Le nœud principal est toujours valide.

La colonne priorité indique la position des nœuds de réplica en relation avec le nœud principal. Le nœud principal ne dispose d'aucune valeur de priorité. Lorsqu'un nœud de réplica est promu nœud principal, sélectionnez le nœud avec la valeur de priorité la plus basse.

Lors de l'utilisation en mode synchrone, vRealize Automation appelle le basculement automatique. En cas de panne du nœud principal, le nœud de réplica suivant disponible devient automatiquement le nouveau principal. L'opération de basculement nécessite 10 à 30 secondes sur un déploiement vRealize Automation classique.

Conditions préalables

- Installez et configurez vRealize Automation conformément aux instructions appropriées fournies dans la section *Installation de vRealize Automation*.
- 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.

- Configurez un cluster de base de données du dispositif Postgres intégré dans le cadre de votre déploiement de vRealize Automation.

Procédure

- 1 Dans l'interface VAMI (Virtual Appliance Management Interface), sélectionnez **Paramètres vRA > Base de données**.
- 2 Si votre base de données utilise plusieurs nœuds, consultez le tableau situé au bas de la page pour vous assurer que le système fonctionne correctement.
 - Vérifiez que tous les nœuds sont indiqués.
 - Assurez-vous que le nœud approprié est le nœud principal désigné.

Note Ne cliquez pas sur le bouton **Mode de synchronisation** pour modifier le mode de synchronisation de la base de données, sauf si vous êtes certain que vos données sont sécurisées. La modification du mode de synchronisation sans préparation peut provoquer une perte de données.

- 3 Pour promouvoir un des nœuds en nœud principal, cliquez sur **Promouvoir** dans la colonne appropriée.
- 4 Cliquez sur **Enregistrer les paramètres** pour enregistrer votre configuration si vous avez effectué des modifications.

Scénarios de basculement automatique à trois nœuds de la base de données du dispositif

Il existe plusieurs scénarios de basculement de haute disponibilité de la base de données du dispositif et le comportement de vRealize Automation varie en fonction de la configuration de la base de données du dispositif et du nombre de nœuds qui échouent.

Scénarios de panne de nœud unique

Si un des trois nœuds échoue, vRealize Automation démarrera un basculement automatique. Aucune opération de basculement automatique supplémentaire ne peut se produire tant que les trois nœuds ne sont pas restaurés.

Le tableau suivant décrit le comportement et les actions associées à une panne de nœud principal dans un déploiement à haute disponibilité.

Tableau 1-5. Échec du nœud principal

| | |
|----------------------|---|
| Comportement attendu | <ul style="list-style-type: none"> ■ Le nœud de réplica de synchronisation configuré devient l'instance principale de et sélectionne automatiquement la fonctionnalité de base de données du dispositif. ■ Le réplica de synchronisation potentiel devient le nœud de synchronisation en attente. ■ Le déploiement de vRealize Automation fonctionne en mode lecture seule jusqu'à ce que le basculement automatique se termine. |
| Autre action | <ul style="list-style-type: none"> ■ Lorsque l'ancien nœud principal est récupéré, il est réinitialisé automatiquement en tant que réplica par la logique de réparation de l'agent de basculement. Aucune action manuelle n'est requise. ■ Si l'ancien nœud principal ne peut pas être récupéré, définissez manuellement la base de données du dispositif sur le mode asynchrone. |

Le tableau suivant décrit le comportement et les actions associées à une panne d'un nœud de réplica de synchronisation dans un déploiement à haute disponibilité.

Tableau 1-6. Échec du réplica de synchronisation

| | |
|----------------------|---|
| Comportement attendu | <ul style="list-style-type: none"> ■ Le déploiement de vRealize Automation ne rencontre pas d'interruption de service. Il y aura un retard de quelques secondes pour les demandes de base de données jusqu'à ce que le réplica potentiel devienne le nouveau réplica de synchronisation. La base de données du dispositif effectue cette action automatiquement. |
| Autre action | <ul style="list-style-type: none"> ■ Lorsque l'ancien réplica de synchronisation se met en ligne, il devient automatiquement un réplica potentiel. Aucune action manuelle n'est requise. ■ Si l'ancien réplica de synchronisation ne peut pas être réparé, définissez manuellement la base de données du dispositif sur le mode asynchrone. |

Le tableau suivant décrit le comportement et les actions associées à une panne de nœud principal dans un déploiement à haute disponibilité.

Tableau 1-7. Échec du réplica potentiel

| | |
|----------------------|--|
| Comportement attendu | Aucune interruption de service du déploiement. |
| Autre action | <ul style="list-style-type: none"> ■ Lorsque l'ancien réplica potentiel se met en ligne, il devient automatiquement un réplica potentiel. Aucune action manuelle n'est requise. ■ Si l'ancien réplica potentiel ne peut pas être réparé, définissez la base de données du dispositif sur le mode asynchrone. |

Scénarios de panne de deux nœuds

Si deux des trois nœuds échouent simultanément, vRealize Automation passe en mode lecture seule jusqu'à ce qu'une réparation manuelle soit effectuée.

Le tableau suivant décrit le comportement et les actions associées à un nœud principal et la panne d'un nœud de réplica potentiel dans un déploiement à haute disponibilité.

Tableau 1-8. Échec du nœud principal et du réplica potentiel

| | |
|----------------------|---|
| Comportement attendu | <ul style="list-style-type: none"> ■ Le réplica de synchronisation n'est pas promu automatiquement à nœud principal. vRealize Automation fonctionne en mode lecture seule, car il peut traiter des transactions en lecture seule jusqu'à ce qu'une promotion manuelle soit effectuée. |
| Autre action | <ul style="list-style-type: none"> ■ Une promotion manuelle est requise. Définissez la base de données du dispositif sur le mode asynchrone. ■ Lorsque le nœud principal et réplica potentiel sont récupérés, définissez-les manuellement pour les synchroniser avec le nouveau nœud principal. À ce stade, vous pouvez faire basculer vRealize Automation vers le mode synchrone. ■ Lorsque deux des trois nœuds sont hors service simultanément, vRealize Automation bascule en mode lecture seule jusqu'à ce qu'une réparation manuelle soit effectuée. Si un seul nœud de base de données est disponible, basculez votre déploiement en mode asynchrone. |

Le tableau suivant décrit le comportement et les actions associées à une panne d'un nœud potentiel et de synchronisation dans un déploiement à haute disponibilité.

Tableau 1-9. Échec des réplicas potentiel et de synchronisation

| | |
|----------------------|--|
| Comportement attendu | <ul style="list-style-type: none"> ■ vRealize Automation fonctionne en mode lecture seule, car il peut traiter les transactions en lecture seule jusqu'à ce qu'une réparation manuelle soit effectuée. |
| Autre action | <ul style="list-style-type: none"> ■ Une promotion manuelle est requise. Définissez la base de données du dispositif sur le mode asynchrone. ■ Lorsque les réplicas potentiel et de synchronisation sont récupérés, ils doivent être réinitialisés manuellement pour se synchroniser avec le nœud principal. À ce stade, vous pouvez faire basculer vRealize Automation vers le mode synchrone. ■ Lorsque deux des trois nœuds sont hors service simultanément, vRealize Automation bascule en mode lecture seule jusqu'à ce qu'une réparation manuelle soit effectuée. Si un seul nœud de base de données est disponible, basculez votre déploiement en mode asynchrone. |

Pannes de liens entre les nœuds

En cas de panne de liens entre les nœuds sur un déploiement distribué, l'agent de basculement automatique tente de réparer la configuration.

Le tableau suivant décrit le comportement et les actions associés à une panne de liens entre deux sites dans un déploiement à haute disponibilité avec la configuration spécifiée lorsque tous les nœuds restent actifs et en ligne.

Site A : principal et réplica potentiel

Site B : réplica de synchronisation

Tableau 1-10. Panne de liens entre deux sites lorsque tous les nœuds restent actifs et en ligne

| | |
|----------------------|---|
| Comportement attendu | Pas d'interruption de service pour le déploiement de vRealize Automation. Le réplica potentiel devient automatiquement le réplica de synchronisation. |
| Autre action | Aucune action manuelle n'est requise. |

Le tableau suivant décrit le comportement et les actions associés à une panne de liens entre deux sites dans un déploiement à haute disponibilité avec la configuration spécifiée lorsque tous les nœuds restent actifs et en ligne.

Site A : principal

Site B : réplica de synchronisation et potentiel

Tableau 1-11. Panne de liens entre deux sites lorsque tous les nœuds restent actifs et en ligne - Autre configuration

| | |
|----------------------|--|
| Comportement attendu | Le réplica de synchronisation devient nœud principal et relève automatiquement les fonctionnalités de base de données du dispositif. L'agent de basculement automatique améliore le réplica potentiel pour devenir le nouveau réplica de synchronisation. Le déploiement de vRealize Automation fonctionne en mode lecture seule jusqu'à ce que cette promotion soit terminée. |
| Autre action | Aucune action manuelle n'est requise. Lorsque le lien est récupéré, l'agent de basculement automatique réinitialise l'ancien nœud principal en tant que réplica. |

Scénario : réaliser un basculement manuel de base de données de dispositif vRealize Automation

En cas de problème avec la base de données Postgres du dispositif vRealize Automation, effectuez un basculement manuel vers un nœud de dispositif réplica vRealize Automation dans le cluster.

En cas de défaillance ou d'arrêt de la base de données Postgres sur le nœud principal du dispositif vRealize Automation, appliquez la procédure suivante.

Note Dès qu'un nœud passe en état défectueux, ne tentez pas d'utiliser son interface de gestion de dispositifs virtuels pour des opérations, notamment le basculement.

Conditions préalables

- Configurez un cluster des nœuds du dispositif vRealize Automation. Chaque nœud héberge une copie de la base de données de dispositif Postgres intégrée.

Procédure

- 1 Supprimez l'adresse IP du nœud principal de l'équilibrage de charge externe.

- 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 **Cluster**.

- 4 Dans la liste des nœuds de réplica, localisez celui qui a la priorité la plus élevée.

Les nœuds de réplica apparaissent par ordre de priorité croissant.

- 5 Cliquez sur **Promouvoir** et attendez que l'opération soit terminée.

Lorsque vous avez terminé, le nœud de réplica est répertorié comme le nouveau nœud principal.

- 6 Corrigez les problèmes avec l'ancien nœud principal et rajoutez-le au cluster :

- a Isolez l'ancien nœud principal.

Déconnectez le nœud de son réseau actuel, c'est-à-dire celui qui achemine vers les autres nœuds du dispositif vRealize Automation. Sélectionnez une autre carte réseau pour la gestion ou gérez-la directement depuis la console de gestion des machines virtuelles.

- b Récupérez l'ancien nœud principal.

Mettez le nœud sous tension ou corrigez l'erreur. Par exemple, vous devez réinitialiser la machine virtuelle si elle ne répond pas.

- c Depuis une session de console en tant qu'utilisateur racine, arrêtez le service vpostgres.

```
service vpostgres stop
```

- d Ajoutez à nouveau l'ancien nœud principal à son réseau d'origine, c'est-à-dire celui qui achemine les données vers les autres nœuds du dispositif vRealize Automation.

- e Depuis une session de console en tant qu'utilisateur racine, redémarrez le service haproxy.

```
service haproxy restart
```

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

- g Sélectionnez **Cluster**.

- h Localisez l'ancien nœud principal et cliquez sur **Réinitialiser**.

- i Après une réinitialisation réussie, redémarrez l'ancien nœud principal.

- j L'ancien nœud principal étant sous tension, vérifiez que les services suivants sont exécutés.

```
haproxy horizon-workspace rabbitmq-server vami-lighttpd vcac-server vco-server
```


- k Ajoutez à nouveau l'ancien nœud principal à l'équilibrage de charge externe.

Note Si un nœud principal qui a été dégradé au rang de réplica est toujours répertorié comme nœud principal, vous devez le joindre à nouveau au cluster manuellement pour corriger le problème.

Scénario : réaliser un basculement de base de données de maintenance

En tant qu'administrateur système vRealize Automation, vous devez réaliser une opération de basculement de maintenance de base de données de dispositif.

Ce scénario considère que le nœud principal actif fonctionne et est exécuté normalement. Il existe deux étapes de maintenance de basculement de base de données : maintenance de l'instance principale de et de la maintenance d'un nœud de réplica. Lorsque qu'un nœud principal a été remplacé pour devenir un réplica, vous devez effectuer des opérations de maintenance sur celui-ci afin qu'il soit en mesure de redevenir le nœud principal si besoin est.

Note Lorsque vous effectuez un basculement de maintenance, n'arrêtez ni ne redémarrez pas le service HAProxy sur la machine hôte concernée.

Conditions préalables

- vRealize Automation est installé et configuré selon les instructions appropriées de *Installation de vRealize Automation*.
- 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.
- Installez et configurez un cluster intégré de base de données des dispositifs Postgres approprié.
- Si votre base de données utilise un mode de réplication synchrone, assurez-vous que le cluster comprend trois nœuds actifs.

Procédure

- 1 Supprimez l'adresse IP du nœud principal de l'équilibrage de charge externe.
- 2 Isolez le nœud principal.

Déconnectez le nœud à partir de son réseau actuel. Il devrait s'agir du réseau qui effectue le routage vers les autres nœuds dispositif vRealize Automation.
- 3 Sélectionnez une autre carte réseau pour la gestion ou gérez-la directement depuis l'interface de gestion des machines virtuelles.
- 4 Sélectionnez le **Cluster** sur l'Interface de gestion de dispositif virtuel.

- 5 Sélectionnez le nœud de réplica avec la priorité la plus basse pour la promotion vers le nœud principal, puis cliquez sur **Promouvoir**.

Les nœuds de réplica apparaissent par ordre de priorité croissant.

L'ancien nœud principal est rétrogradé au rang de réplica et le nouveau nœud principal est promu.

- 6 Réalisez les actions de maintenance de réplica appropriées.
- 7 Lorsque la maintenance est terminée, assurez-vous que le dispositif virtuel fonctionne, est connecté au réseau et que son service HAProxy est exécuté.
 - a Connectez-vous à la console de gestion vRealize Automation en tant qu'utilisateur **racine**.
 - b Assurez-vous le nœud de réplica peut faire l'objet d'une commande Ping, qu'il peut être résolu par son nom et que son état est récent sur l'onglet **Cluster** d'interface de gestion de dispositifs virtuels.
- 8 Cliquez sur **Réinitialiser** pour le nœud de réplica.

Cette opération réinitialise la base de données afin qu'elle soit configurée pour répliquer le nœud principal actif et resynchroniser le nœud de réplica avec la dernière configuration haproxy du nœud principal.

- 9 Après la réinitialisation, renvoyez l'adresse IP du nœud de réplica du dispositif virtuel au pool d'adresse IP de l'équilibrage de charge du dispositif virtuel externe.
- 10 Assurez-vous que le nœud de réplica est sain dans la table de base de données, qu'il peut faire l'objet d'une commande Ping et qu'il peut être résolu par son nom.

Étape suivante

Corrigez les problèmes avec l'ancien nœud principal et rajoutez-le au cluster.

Récupérer manuellement la base de données de dispositif d'une défaillance irrémédiable

Si la base de données de dispositif tombe en panne et qu'aucun nœud de base de données n'est actif et en cours d'exécution, ou si tous les nœuds de réplica sont désynchronisés lorsque le nœud principal échoue, procédez comme suit pour tenter de récupérer la base de données.

Cette procédure s'applique aux situations dans lesquelles aucun nœud de base de données n'est opérationnel sur un cluster s'exécutant en mode asynchrone. Dans ce scénario, vous voyez généralement des erreurs similaires aux erreurs suivantes sur la page de l'interface de gestion de dispositif virtuel lors d'une tentative de chargement ou d'actualisation de la page :

```
Erreur d'initialisation du service de base de données : impossible d'ouvrir la connexion JDBC pour transaction ; l'exception imbriquée est org.postgresql.util.PSQLException : Échec de la tentative de connexion.
```

Procédure

- 1 Essayez de restaurer la base de données à l'aide de l'interface de gestion de dispositif virtuel à partir de l'un des nœuds de base de données.
 - a Si possible, ouvrez la page **Cluster** de l'interface de gestion de dispositif virtuel du nœud présentant l'état le plus récent. En général, ce nœud est celui qui était le nœud principal avant l'échec de la base de données.
 - b Si l'interface de gestion de dispositif virtuel pour le nœud principal ne parvient pas à s'ouvrir, essayez d'ouvrir l'interface pour d'autres nœuds de réplica.
 - c Si vous pouvez trouver un nœud de base de données avec une interface de gestion de dispositif virtuel opérationnelle, essayez de le récupérer en effectuant un basculement manuel.

Reportez-vous à [Scénario : réaliser un basculement manuel de base de données de dispositif vRealize Automation](#).

- 2 En cas d'échec de la procédure de l'étape 1, démarrez une session de shell et tentez de déterminer le nœud ayant l'état le plus récent. Ouvrez une session de shell dans tous les nœuds de cluster disponibles et essayez de démarrer leurs bases de données en exécutant la commande shell suivante : `service vpostgres start`
- 3 Utilisez la procédure suivante pour chaque nœud qui a une base de données locale en cours d'exécution pour déterminer le nœud ayant l'état le plus récent.
 - a Exécutez la commande suivante pour déterminer le nœud ayant l'état le plus récent : Si la commande renvoie `f`, le nœud est celui ayant l'état le plus récent et vous pouvez continuer à l'étape 4.

```
su - postgres
psql vcac
vcac=# select pg_is_in_recovery();
pg_is_in_recovery
```

- Si cette commande renvoie `f`, ce nœud a l'état le plus récent.
- Si le nœud renvoie `t`, exécutez-y la commande suivante :

```
SELECT pg_last_xlog_receive_location() as receive_loc, pg_last_xlog_replay_location() as
replay_loc, extract(epoch from pg_last_xact_replay_timestamp()) as replay_timestamp;
```

Cette commande doit renvoyer un résultat semblable à ce qui suit.

```
vcac=# SELECT pg_last_xlog_receive_location() as receive_loc, pg_last_xlog_replay_location()
as replay_loc, extract(epoch from pg_last_xact_replay_timestamp()) as replay_timestamp;
 receive_loc | replay_loc | replay_timestamp
-----+-----+-----
 0/20000000 | 0/203228A0 | 1491577215.68858
(1 row)
```

- 4 Comparez les résultats pour chaque nœud afin de déterminer celui qui a l'état le plus récent.

Sélectionnez le nœud possédant la valeur la plus élevée sous la colonne `receive_loc`, en cas d'égalité, sélectionnez la valeur la plus élevée dans la colonne `replay_loc`, puis en cas de nouvelle égalité, sélectionnez le nœud possédant la valeur `replay_timestamp` la plus élevée.

- 5 Exécutez la commande suivante sur le nœud ayant l'état le plus récent : `vcac-vami psql-promote-master -force`
- 6 Ouvrez le fichier `/etc/haproxy/conf.d/10-psql.cfg` dans un éditeur de texte et mettez à jour la ligne suivante

```
server masterserver sc-rdops-vm06-dhcp-170-156.eng.vmware.com:5432 check on-marked-up shutdown-backup-sessions
```

Elle doit correspondre au nom de domaine complet du nœud actuel :

```
server masterserver current-node-fqdn:5432 check on-marked-up shutdown-backup-sessions
```

- 7 Enregistrez le fichier.
- 8 Exécutez la commande `service haproxy restart`.
- 9 Ouvrez la page **Cluster** de l'interface de gestion de dispositifs virtuels pour le nœud plus récent.

Ce nœud doit être indiqué comme nœud principal et les autres nœuds comme réplicas non valides. En outre, le bouton **Réinitialiser** pour les réplicas doit être activé.
- 10 Cliquez sur **Réinitialiser** successivement pour chaque réplica jusqu'à ce que l'état du cluster soit réparé.

Sauvegarde et récupération d'installations de vRealize Automation

Afin de minimiser les arrêts système et les pertes de données en cas de panne, les administrateurs sauvegardent régulièrement l'installation entière de vRealize Automation. Si votre système échoue, vous pouvez récupérer en restaurant la dernière sauvegarde connue et en réinstallant certains composants.

Pour sauvegarder et restaurer vRealize Automation, consultez les rubriques suivantes de la [documentation vRealize Suite](#) :

- vRealize Automation Préparatifs pour la sauvegarde
- Restauration du système vRealize Automation

Programme d'amélioration de l'expérience utilisateur

Ce produit fait partie du Programme d'amélioration de l'expérience utilisateur de VMware. Grâce à ce programme, VMware dispose d'informations permettant à VMware d'améliorer ses produits

et services, de corriger les problèmes et de vous fournir des conseils sur la meilleure façon de déployer et d'utiliser nos produits. Vous pouvez rejoindre ou quitter ce programme pour vRealize Automation à tout moment.

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>.

Rejoindre ou quitter le Programme d'amélioration du produit de vRealize Automation

Vous pouvez rejoindre ou quitter le Programme d'amélioration du produit (CEIP) de vRealize Automation à tout moment.

vRealize Automation vous permet de rejoindre le Programme d'amélioration du produit (CEIP) lors de l'installation et de la configuration initiales du produit. Après l'installation, vous pouvez rejoindre ou quitter le CEIP en suivant la procédure suivante.

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 **Télémétrie**.
- 3 Cochez ou décochez l'option **Rejoindre le Programme d'amélioration du produit de VMware**.
Lorsqu'elle est cochée, l'option active le programme et envoie les données à `https://vmware.com`.
- 4 Cliquez sur **Enregistrer les paramètres**.

Configurer l'heure de collecte des données

Vous pouvez définir le jour et l'heure auxquels le Programme d'amélioration du produit envoie des données à VMware.

Procédure

- 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.
`/etc/telemetry/telemetry-collector-vami.properties`

- 3 Modifiez les propriétés pour le jour de la semaine (dow) et l'heure du jour (hod).

| Propriété | Description |
|------------------------------------|---|
| frequency.dow=<jour de la semaine> | Jour de la collecte de données. |
| frequency.hod=<heure du jour> | Heure locale du jour de collecte des données. Les valeurs possibles vont de 0 à 23. |

- 4 Enregistrez et fermez `telemetry-collector-vami.properties`.

- 5 Appliquez les paramètres en entrant la commande suivante.

```
vcac-config telemetry-config-update --update-info
```

Les modifications s'appliquent à l'ensemble des nœuds de votre déploiement.

Ajustement des paramètres système

En votre qualité d'administrateur système, vous ajustez la journalisation et personnalisez les modèles d'e-mails IaaS. Vous pouvez également gérer les paramètres qui s'affichent par défaut pour chaque locataire (comme les serveurs de messagerie électronique devant gérer les notifications). Les administrateurs de locataire peuvent remplacer ces paramètres par défaut si nécessaire.

Modifier l'icône Tous les services dans le catalogue de services

Vous pouvez modifier l'icône par défaut du catalogue de services pour afficher une image personnalisée. Lorsque vous modifiez l'icône, cette modification s'applique à tous les locataires. Vous ne pouvez pas configurer des icônes spécifiques à un locataire pour le catalogue.

Des commandes sont fournies pour Linux ou Mac et Windows afin que vous puissiez exécuter les commandes cURL sur tous ces systèmes d'exploitation.

Conditions préalables

- Convertissez l'image en une chaîne codée de base64.
- cURL doit être installé sur la machine sur laquelle vous exécutez les commandes.
- Vous devez disposer des informations d'identification d'un utilisateur de vRealize Automation ayant le rôle d'administrateur système.

Procédure

- 1 Définissez la variable VCAC dans la session de terminal pour les commandes cURL.

| Système d'exploitation | Commande |
|------------------------|---|
| Linux/Mac | <code>export VCAC=<VA URL></code> |
| Windows | <code>set VCAC=<VA URL></code> |

2 Récupérez le jeton d'authentification pour l'utilisateur administrateur système.

| Système d'exploitation | Commande |
|------------------------|---|
| Linux/Mac | <pre>curl https://\$VCAC/identity/api/tokens --insecure -H "Accept: application/json" -H 'Content-Type: application/json' --data '{"username":"<Catalog Administrator User>","password":"<password>","tenant":"vsphere.local"}'</pre> |
| Windows | <pre>curl https://%VCAC%/identity/api/tokens --insecure -H "Accept:application/json" -H "Content-Type:application/json" --data "{\"username\":\"<Catalog Administrator User>\",\"password\":\"<password>\",\"tenant\":\"vsphere.local\"}"</pre> |

Un jeton d'authentification est généré.

3 Définissez la variable du jeton d'authentification en remplaçant <Auth Token> par la chaîne du jeton que vous avez généré à l'étape précédente.

| Système d'exploitation | Commande |
|------------------------|--|
| Linux/Mac | <pre>export AUTH="Bearer <Auth Token>"</pre> |
| Windows | <pre>set AUTH=Bearer <Auth Token></pre> |

4 Ajoutez la chaîne codée de base64 pour l'image.

| Système d'exploitation | Commande |
|------------------------|---|
| Linux/Mac | <pre>curl https://\$VCAC/catalog-service/api/icons --insecure -H "Accept: application/json" -H 'Content-Type: application/json' -H "Authorization: \$AUTH" --data '{"id":"cafe_default_icon_genericAllServices","fileName":"<filename>","contentType":"image/png","image":"<IMAGE DATA as base64 string>"}</pre> |
| Windows | <pre>curl https://%VCAC%/catalog-service/api/icons --insecure -H "Accept: application/json" -H "Content-Type: application/json" -H "Authorization: %AUTH%" --data "{\"id\":\"cafe_default_icon_genericAllServices\",\"fileName\":\"<filename>\",\"contentType\":\"image/png\",\"image\":\"<IMAGE DATA as base64 string>\"}"</pre> |

Résultats

L'icône des nouveaux services s'affiche dans le catalogue des services après environ cinq minutes.

Si vous voulez revenir à l'icône par défaut, vous pouvez exécuter la commande suivante après avoir suivi les étapes 1 à 3.

| Système d'exploitation | Commande |
|------------------------|--|
| Linux/Mac | <pre>curl https://\$VCAC/catalog-service/api/icons/cafe_default_icon_genericAllServices --insecure -H "Authorization: \$AUTH" --request DELETE</pre> |
| Windows | <pre>curl https://%VCAC%/catalog-service/api/icons/cafe_default_icon_genericAllServices --insecure -H "Authorization: %AUTH%" --request DELETE</pre> |

Personnaliser les paramètres de rotation des données

Vous pouvez configurer les paramètres de rotation des données de vRealize Automation afin de contrôler la façon dont le système conserve, archive et supprime les données héritées.

La fonctionnalité de rotation des données permet d'activer la rotation des données, de configurer le nombre maximal de jours pendant lesquels vRealize Automation doit conserver des données dans la base de données SQL Server IaaS avant leur archivage ou leur suppression, et bien d'autres contrôles de rotation des données.

Par défaut, la fonctionnalité de survol des données est désactivée.

Pour configurer les paramètres de rotation des données, accédez à la page **Paramètres globaux** de vRealize Automation. Une fois activée, la fonctionnalité interroge des données et les supprime des tables de la base de données SQL Server suivantes :

- UserLog
- Audit
- CategoryLog
- VirtualMachineHistory
- VirtualMachineHistoryProp
- AuditLogItems
- AuditLogItemsProperties
- TrackingLogItems
- WorkflowHistoryInstances
- WorkflowHistoryResults

Si vous définissez le paramètre `DataRolloverIsArchiveEnabled` sur `True`, des versions archivées des tables sont créées dans le schéma `dbo`. Par exemple, la version archivée de `UserLog` est `UserLogArchive` et la version archivée de `VirtualMachineHistory` est `VirtualMachineHistoryArchive`.

Lorsqu'elle est activée, la fonctionnalité de rotation des données s'exécute une fois par jour à 03 h 00 (heure prédéterminée), selon la configuration du fuseau horaire du dispositif vRealize Automation. Le paramètre `DataRollover MaximumAgeInDays` permet de définir le nombre maximal de jours pendant lesquels les données doivent être conservées. En général, ce processus s'exécute rapidement et prend de quelques minutes à une heure. Toutefois, lorsque cette fonctionnalité est activée pour la première fois, le processus peut avoir un grand nombre

de données à récupérer pour l'archivage ou la suppression, et ainsi prendre beaucoup plus de temps. Le processus est conçu pour s'exécuter jusqu'à ce qu'il ait fini. Il exécute ses travaux par lots, composés de blocs transactionnels petits et rapides, afin ne pas causer de problèmes de simultanéité. Notez que ce processus peut être arrêté normalement comme décrit ci-dessous.

Note Pour arrêter le processus DataRollover, remplacez le paramètre `DataRollover Status` de `En cours d'exécution` par `Désactivé` ou `Activé`. Le processus en cours d'exécution s'arrête normalement. Aucune tâche n'est perdue. Toutes les données archivées ou supprimées jusqu'au point d'arrêt du processus sont enregistrées.

Si le paramètre `DataRollover IsArchiveEnabled` est défini sur `True`, les données antérieures au nombre de jours spécifiés dans le paramètre `DataRollover MaximumAgeInDays` sont déplacées vers les tables d'archivage. Si le paramètre `DataRollover IsArchiveEnabled` est défini sur `False`, les données sont définitivement supprimées sans aucun archivage. Une fois supprimées, les données ne sont pas récupérables.

Procédure

- 1 Connectez-vous à la console de vRealize Automation en tant qu'**administrateur système**.
- 2 Sélectionnez **Infrastructure > Administration > Paramètres globaux**.
- 3 Sur la page **Paramètres globaux**, localisez dans la table la section **Rotation des données**. Examinez les paramètres et configurez-les.

| Configuration | Description |
|--|--|
| <code>DataRollover BatchSize</code> | Ce paramètre est défini par défaut sur 2 000 et n'a généralement pas besoin d'être modifié. Cependant, si vous constatez une baisse des performances, une valeur plus petite pour <code>BatchSize</code> peut aider. Une valeur plus grande pour <code>BatchSize</code> peut accélérer l'exécution de la tâche, mais accroît la pression sur le traitement simultané. La plage valide est comprise entre 100 et 20 000. |
| <code>DataRollover IsArchiveEnabled</code> | Spécifie si les données de rotation doivent être déplacées vers les tables d'archivage après que le nombre maximal de jours a été atteint. Par défaut, cette valeur est définie sur <code>True</code> . Si vous définissez cette valeur sur <code>False</code> , toutes les données antérieures à la valeur spécifiée dans le paramètre <code>DataRollover MaximumAgeInDays</code> sont définitivement supprimées. |
| <code>DataRollover MaximumAgeInDays</code> | Spécifie le nombre maximal de jours pendant lesquels le système conserve les données dans la base de données, avant de les déplacer vers l'archive ou de les supprimer définitivement. Par défaut, cette valeur est définie sur 90 jours. |

| Configuration | Description |
|--|--|
| DataRollover Status | Spécifie si la rotation des données doit être activée. Par défaut, ce paramètre est défini sur Désactivé. Pour activer la fonctionnalité, définissez ce paramètre sur Activé. |
| DataRollover VirtualMachineHistory BatchSize | Spécifie la taille du lot dans la table VirtualMachineHistory, dans la plage d'enregistrements allant de 1 à 5. La valeur par défaut est 1. |
| DataRollover UpdateStatistics | Le paramètre UpdateStatistics est désactivé par défaut, mais il est fortement recommandé de l'activer (le définir sur 1), car les statistiques mises à jour sont bonnes pour les performances de la requête. Cela force la procédure stockée [dbo].[usp_DataRollover] à exécuter une commande update statistics sur les tables après l'exécution du processus d'archivage. |

- 4 Dans la première colonne de la table, cliquez sur l'icône **Modifier** (✎) pour modifier un paramètre.

La zone **Valeur** pour le paramètre correspondant devient modifiable.

- 5 Dans la première colonne de la table, cliquez sur l'icône **Enregistrer** (✓) pour enregistrer les modifications apportées.

Ajustement des paramètres du fichier de configuration du service de gestionnaire

Vous pouvez utiliser le fichier de configuration du service de gestionnaire (managerService.exe.config) pour ajuster des paramètres communs de déploiements de machine.

Le fichier managerService.exe.config réside généralement dans l'annuaire %System-Drive%\Program Files x86\VMware\vCAC\Server. Il est préférable de toujours réaliser une copie du fichier avant de le modifier.

Vous pouvez utiliser les paramètres du fichier suivant managerService.exe.config afin de contrôler les divers aspects des déploiements de machine. Les valeurs par défaut sont affichées.

- `<add key="ProcessLeaseWorkflowTimerCallbackIntervalMilliseconds" value="3600000"/>`
- `<add key="BulkRequestWorkflowTimerCallbackMilliseconds" value="10000"/>`
- `<add key="MachineRequestTimerCallbackMilliseconds" value="10000"/>`
- `<add key="MachineWorkflowCreationTimerCallbackMilliseconds" value="10000"/>`
- `<add key="RepositoryConnectionMaxRetryCount" value="100"/>`
- `<add key="MachineCatalogRegistrationRetryTimerCallbackMilliseconds" value="120000"/>`
- `<add key="MachineCatalogUnregistrationRetryTimerCallbackMilliseconds" value="120000"/>`

- `<add key="MachineCatalogUpdateMaxRetryCount" value="15"/>`

Définition de limites de simultanéité exigeantes en ressources

Pour conserver vos ressources, vRealize Automation limite le nombre d'instances de provisionnement de machines et de collecte de données exécutées simultanément. Vous pouvez modifier les limites.

Configuration de provisionnement de machine simultané

Plusieurs demandes simultanées de provisionnement de machine peuvent impacter les performances de vRealize Automation. Vous pouvez apporter des modifications aux limites placées sur les agents proxy et les activités du workflow afin d'altérer les performances.

En fonction des besoins des propriétaires de machines de votre site, le serveur vRealize Automation peut recevoir plusieurs demandes simultanées de provisionnement de machine. Cela peut se produire dans les cas suivants :

- Un seul utilisateur envoie une demande pour plusieurs machines.
- De nombreux utilisateurs demandent des machines en même temps.
- Un ou plusieurs gestionnaires de groupes approuvent plusieurs demandes de machines en attente de façon très rapprochée.

La durée nécessaire à vRealize Automation pour provisionner une machine augmente généralement lorsque le nombre de demandes simultanées s'élève. L'augmentation de la durée de provisionnement dépend de trois facteurs importants :

- L'effet sur les performances des activités de workflow vRealize Automation simultanées et gourmandes en ressources, y compris l'activité SetupOS (pour les machines créées au sein de la plate-forme de virtualisation, de même que dans le provisionnement basé sur WIM) et l'activité Cloner (pour les machines clonées au sein de la plate-forme de virtualisation).
- La limite vRealize Automation configurée sur le nombre d'activités de provisionnement gourmandes en ressources (généralement longues) qui peuvent être exécutées de façon simultanée. La valeur par défaut est 8. Les activités simultanées au-delà de la limite configurée sont mises en file d'attente.
- Toute limite au sein de la plate-forme de virtualisation ou du compte de service cloud sur le nombre d'éléments de travail vRealize Automation (gourmands en ressources ou non) qui peuvent être exécutés de façon simultanée. Par exemple, la limite par défaut dans vCenter Server est égale à 4, les éléments de travail supplémentaires étant mis en file d'attente.

Par défaut, vRealize Automation limite les activités de provisionnement virtuelles simultanées pour les hyperviseurs qui utilisent des agents proxy à 8 par point de terminaison. Cela permet de garantir que la plate-forme de virtualisation gérée par un agent particulier ne reçoit pas suffisamment d'éléments de travail gourmands en ressources pour éviter l'exécution d'autres

éléments. Envisagez de tester soigneusement les effets d'une modification de la limite avant d'effectuer des modifications. Pour définir la meilleure limite pour votre site, vous pouvez avoir à examiner l'exécution des éléments de travail au sein de la plate-forme de virtualisation ainsi que l'exécution des activités de workflow au sein de vRealize Automation.

Si vous augmentez la limite vRealize Automation configurée par agent, vous devrez peut-être réaliser des ajustements de configuration supplémentaires dans vRealize Automation, comme suit :

- Les délais d'exécution par défaut des activités de workflow SetupOS et Cloner sont de deux heures chacun. Si le temps requis pour exécuter l'une de ces activités dépasse cette limite, l'activité est annulée et le provisionnement échoue. Pour empêcher cet échec, augmentez l'un de ces délais d'exécution ou les deux.
- Les délais d'expiration de livraison pour les activités de workflow SetupOS et Cloner sont de 20 heures chacun. Une fois que l'une de ces activités est initiée, si la machine résultant de l'activité n'a pas été provisionnée dans les 20 heures, l'activité est annulée et le provisionnement échoue. Par conséquent, si vous avez augmenté la limite au point où cette situation se produit parfois, vous devrez augmenter l'un de ces délais d'expiration de livraison ou les deux.

Configuration de collectes de données simultanées

Par défaut, vRealize Automation limite les activités de collecte de données simultanées. Si vous modifiez cette limite, vous pouvez empêcher les expirations inutiles en modifiant les délais d'exécution par défaut des différents types de collectes de données.

vRealize Automation collecte régulièrement des données auprès de ressources de calcul de virtualisation connues via ses agents proxy et auprès des comptes du service cloud et des machines physiques via les points de terminaison qui les représentent. En fonction du nombre de ressources de calcul de virtualisation, d'agents et de points de terminaison de votre site, des opérations de collecte de données simultanées peuvent avoir lieu fréquemment.

La durée d'exécution des collectes de données dépend du nombre d'objets sur les points de terminaison, notamment les machines virtuelles, les banques de données, les modèles et les ressources de calcul. En fonction de nombreuses conditions, une simple collecte de données peut prendre beaucoup de temps. Comme avec le provisionnement de machine, la simultanéité augmente la durée nécessaire à l'exécution d'une collecte de données.

Par défaut, les activités de collecte de données simultanées sont limitées à deux par agent, les autres étant mises en file d'attente. Ceci permet de garantir que chaque collecte de données s'exécute relativement rapidement et que les activités de collecte de données simultanée sont peu susceptibles d'affecter les performances d'laaS.

En fonction des ressources et des circonstances de votre site, il est toutefois possible d'élever la limite configurée tout en maintenant une rapidité suffisante pour tirer parti de la simultanéité dans la collecte de données du proxy. L'élévation de la limite peut augmenter également le temps nécessaire à l'exécution d'une simple collecte de données, ce qui peut être compensé par la capacité à collecter d'avantage d'informations d'un plus grand nombre de ressources de calcul et de machines à la fois.

Si vous élevez la limite configurée par-agent, vous devrez peut-être ajuster le délai d'exécution des différents types de collectes de données qui utilisent un agent proxy—inventaire, performance, état et WMI. Si le temps requis pour exécuter l'une de ces activités dépasse le délai d'expiration configuré, l'activité est annulée, puis redémarrée. Pour empêcher l'annulation de l'activité, augmentez un ou plusieurs de ces délais d'exécution.

Ajuster les limites de simultanéité et les délais d'expiration

Vous pouvez modifier les limites par agent du provisionnement simultané, des activités de collecte de données, ainsi que les délais d'expiration par défaut.

Lorsque vous tapez une valeur par défaut pour ces variables, utilisez le format hh:mm:ss (hh=heures, mm=minutes et ss=secondes).

Conditions préalables

Connectez-vous en tant qu'administrateur au serveur hébergeant IaaS Manager Service. Pour les installations distribuées, il s'agit du serveur sur lequel Manager Service a été installé.

Procédure

- 1 Ouvrez le fichier `ManagerService.exe.config` dans un éditeur. Le fichier est localisé dans l'annuaire d'installation du serveur vRealize Automation, généralement `%SystemDrive%\Program Files x86\VMware\VCAC\Server`.
- 2 Localisez la section appelée `workflowTimeoutConfigurationSection`.
- 3 Mettez à jour les variables suivantes, selon les besoins.

| Paramètre | Description |
|---|--|
| <i>MaxOutstandingResourceIntensive WorkItems</i> | Limite de provisionnement simultané (8 par défaut) |
| <i>CloneExecutionTimeout</i> | Délai d'expiration d'exécution du provisionnement virtuel |
| <i>SetupOSExecutionTimeout</i> | Délai d'expiration d'exécution du provisionnement virtuel |
| <i>CloneTimeout</i> | Délai d'expiration de remise de clone de provisionnement virtuel |
| <i>SetupOSTimeout</i> | Délai d'expiration de remise de SE de configuration de provisionnement virtuel |
| <i>CloudInitializeProvisioning</i> | Délai d'expiration d'initialisation de provisionnement cloud |
| <i>MaxOutstandingDataCollectionWorkItems</i> | Limite de collecte de données simultanée |
| <i>InventoryTimeout</i> | Délai d'expiration d'exécution de collecte de données d'inventaire |

| Paramètre | Description |
|---------------------------|--|
| PerformanceTimeout | Délai d'expiration d'exécution de collecte de données de performance |
| StateTimeout | Délai d'expiration d'exécution de collecte de données d'état |

- 4 Enregistrez et fermez le fichier.
- 5 Sélectionnez **Démarrer > Outils d'administration > Services**.
- 6 Arrêtez, puis redémarrez le service vRealize Automation.
- 7 (Facultatif) Si vRealize Automation s'exécute en mode haute disponibilité, toute modification effectuée au fichier `ManagerService.exe.config` après installation doit s'appliquer au serveur principal et au serveur de basculement.

Ajuster la fréquence d'exécution des rappels de machine

Vous pouvez modifier la fréquence de plusieurs procédures de rappel, y compris la fréquence à laquelle la procédure de rappel de vRealize Automation est exécutée pour les baux de machine modifiés.

vRealize Automation utilise un intervalle de temps configuré pour exécuter différentes procédures de rappel sur le service Model Manager, tel que `ProcessLeaseWorkflowTimerCallbackIntervalMiliSeconds` qui recherche les machines dont les baux ont été modifiés. Vous pouvez modifier ces intervalles de temps afin d'augmenter ou de diminuer la fréquence.

Lorsque vous entrez une valeur pour ces variables, entrez une valeur en millisecondes. Par exemple, 10 000 millisecondes = 10 secondes et 3 600 000 millisecondes = 60 minutes = 1 heure.

Conditions préalables

Connectez-vous en tant qu'administrateur au serveur hébergeant IaaS Manager Service. Pour les installations distribuées, il s'agit du serveur sur lequel Manager Service a été installé.

Procédure

- 1 Ouvrez le fichier `ManagerService.exe.config` dans un éditeur. Le fichier est localisé dans l'annuaire d'installation du serveur vRealize Automation, généralement `%SystemDrive%\Program Files x86\VMware\VCAC\Server`.
- 2 Mettez à jour les variables suivantes, selon les besoins.

| Paramètre | Description |
|---|--|
| RepositoryWorkflowTimerCallbackMiliSeconds | Recherche l'activité du service du référentiel ou le service Web Model Manager. La valeur par défaut est 10 000. |
| ProcessLeaseWorkflowTimerCallbackIntervalMiliSeconds | Recherche les baux de machine expirés. La valeur par défaut est 3 600 000. |
| BulkRequestWorkflowTimerCallbackMiliSeconds | Recherche les demandes en bloc. La valeur par défaut est 10 000. |

| Paramètre | Description |
|---|---|
| <i>MachineRequestTimerCallbackMiliSeconds</i> | Recherche les demandes de machine. La valeur par défaut est 10 000. |
| <i>MachineWorkflowCreationTimerCallbackMiliSeconds</i> | Recherche les nouvelles machines. La valeur par défaut est 10 000. |

- 3 Enregistrez et fermez le fichier.
- 4 Sélectionnez **Démarrer > Outils d'administration > Services**.
- 5 Arrêtez, puis redémarrez le service vCloud Automation Center.
- 6 (Facultatif) Si vRealize Automation s'exécute en mode haute disponibilité, toute modification effectuée au fichier `ManagerService.exe.config` après installation doit s'appliquer au serveur principal et au serveur de basculement.

Ajuster les paramètres du journal IaaS

Vous pouvez ajuster vRealize Automation afin d'établir une connexion uniquement avec les informations que vous souhaitez afficher dans le journal de Manager Service.

Si vRealize Automation est exécuté en mode de haute disponibilité, et que vous souhaitez effectuer des modifications dans le fichier `ManagerService.exe.config` après l'installation, vous devez effectuer les modifications sur les serveurs vRealize Automation principal et de basculement.

Procédure

- 1 Connectez-vous au serveur vRealize Automation en utilisant des informations d'identification avec un accès d'administrateur.
- 2 Modifiez le fichier `ManagerService.exe.config` dans `%SystemDrive%\Program Files x86\VMware\VCAC\Server` ou dans le répertoire d'installation de vRealize Automation, s'il est situé dans un emplacement différent.

- 3 Modifiez les clés `RepositoryLogSeverity` et `RepositoryLogCategory` pour déterminer les types d'événements qui doivent être écrits dans les fichiers journaux.

| Option | Description |
|------------------------------|--|
| RepositoryLogSeverity | <p>Spécifiez un niveau de sévérité afin d'ignorer les événements dont le niveau est inférieur à celui indiqué.</p> <ul style="list-style-type: none"> ■ Le niveau <i>Erreur</i> journalise uniquement les erreurs récupérables et les événements d'un niveau supérieur. ■ Le niveau <i>Avertissement</i> journalise les avertissements non critiques et les événements d'un niveau supérieur. ■ Le niveau <i>Informations</i> journalise tous les messages informatifs et les événements d'un niveau supérieur. ■ Le niveau <i>Détaillé</i> journalise une trace de débogage et peut altérer les performances. <p>Par exemple, <code><add key="RepositoryLogSeverity" value="Warning" /></code>.</p> |
| RepositoryLogCategory | <p>Spécifiez une catégorie de journalisation de tous les événements, indépendamment de leur niveau de sévérité. Par exemple, <code><add key="RepositoryLogCategory" value="MissingMachines,UnregisteredMachines,AcceptMachineRequest,RejectMachineRequest" /></code> journalise tous les événements relatifs aux machines manquantes ou désenregistrées, ainsi que toutes les demandes de machine acceptées ou rejetées.</p> |

- 4 Enregistrez et fermez le fichier.
- 5 Sélectionnez **Démarrer > Outils d'administration > Services** et redémarrez le service vCloud Automation Center.

Résultats

Pour connaître l'incidence de vos modifications sur la journalisation, affichez le fichier journal de Manager Service situé dans `%SystemDrive%\Program Files (x86)\VMware\VCAC\Server\Logs` sur la machine où Manager Service est installé, ou dans le répertoire d'installation du serveur, si vous l'avez installé dans un emplacement différent.

Surveillance vRealize Automation

Selon votre rôle, vous pouvez surveiller des workflows ou des services, afficher des journaux d'événement ou d'audit, ou encore collecter des journaux pour tous les hôtes dans un déploiement distribué.

Surveillance des workflows et affichage des journaux

Selon votre rôle, vous pouvez surveiller des workflows et afficher des journaux d'activités.

Tableau 1-12. Options de surveillance et d'affichage des journaux

| Objectif | Rôle | Séquence et description du menu |
|--|---|---|
| Afficher des informations sur les actions ayant eu lieu, comme le type de l'action, la date et l'heure de l'action, etc. | Administrateur IaaS | Permet d'afficher les informations journalisation par défaut ou contrôler l'affichage du contenu à l'aide des options de colonne et de filtre. Sélectionnez Infrastructure > Surveillance > Journal d'audit . Le journal d'audit fournit des détails sur l'état des machines virtuelles gérées et les activités effectuées sur ces machines pendant la reconfiguration. Le journal contient des informations relatives aux actions de provisionnement de machine, de NSX, de récupération et de reconfiguration. |
| Afficher l'état du DEM et autres workflows planifiés et disponibles. | Administrateur IaaS | Permet d'afficher l'état du workflow et, en option, d'ouvrir un workflow spécifique pour en afficher les détails. Sélectionnez Infrastructure > Surveillance > Statut DEM . |
| Afficher et, en option, exporter les données du journal. | Administrateur IaaS | Permet d'afficher les informations journalisation par défaut ou contrôler l'affichage du contenu à l'aide des options de colonne et de filtre. Sélectionnez Infrastructure > Surveillance > Journal . |
| Afficher l'état et l'historique du DEM et d'autres workflows exécutés. | Administrateur IaaS | Permet d'afficher l'historique du workflow et, en option, d'ouvrir un workflow spécifique pour en afficher les détails. Sélectionnez Infrastructure > Surveillance > Historique de workflow . |
| Afficher une liste d'événements, y compris le type de l'événement, son heure, l'ID d'utilisateur, etc. et, en option, afficher la page des détails d'un événement. | Administrateur système | Permet d'afficher une liste d'événements et leurs attributs associés, comme l'heure d'exécution, la description de l'événement, le nom du locataire, le type et l'ID de la cible et d'autres caractéristiques. Sélectionnez Administration > Événements > Journaux des événements . |
| Surveillez l'état de vos demandes et affichez les détails d'une demande. | Administrateur de locataire ou gestionnaire de groupes d'activité | Permet d'afficher l'état des demandes dont vous êtes le responsable ou le propriétaire. Cliquez sur Demandes . |
| Affichez les informations sur les événements récents. | Administrateur IaaS ou administrateur de locataire | Affichez les événements récents pour l'utilisateur actuellement connecté. Sélectionnez Infrastructure > Événements récents |

Surveillance des journaux d'événement et des services

Vous pouvez surveiller les journaux d'événement et les services vRealize Automation pour déterminer leur état actuel et passé.

La période de rétention par défaut des journaux des événements est de 90 jours. Vous pouvez modifier cette période dans le fichier `/etc/vcac/vcac.properties`.

Pour en savoir plus sur l'effacement des journaux en personnalisant les réglages de remplacement de données, consultez *Configuration de vRealize Automation*.

Services vRealize Automation

Un administrateur système peut consulter l'état des services vRealize Automation depuis le journal des événements sur la console de l'administrateur système.

Les sous-ensembles de services sont requis pour exécuter des composants de produits individuels. Par exemple, les services d'identité et les services de cœur d'interface utilisateur doivent être exécutés avant que vous puissiez configurer un locataire.

Les tableaux suivants vous indiquent quels services sont associés avec des secteurs de fonctionnalité vRealize Automation.

Tableau 1-13. groupe Identity Service

| Service | Description |
|--------------------|----------------------------------|
| service de gestion | groupe Identity Service |
| sts-service | Dispositif Single Sign-On |
| autorisation | Service d'autorisation |
| authentification | Authentification |
| eventlog-service | Service de journal d'événement |
| licensing-service | Service d'attribution de licence |

Tableau 1-14. services de cœur d'interface utilisateur

| Service | Description |
|------------------|--|
| shel-ui-app | Service de shell |
| branding-service | Service d'informations de personnalisation |
| plugin-service | Service d'extensibilité (plug-in) |
| portal-service | Service de portail |

Tous les services suivants sont requis pour exécuter le composant IaaS.

Tableau 1-15. Groupe de catalogues de services (services de gouvernance)

| Service | Description |
|----------------------|------------------------------|
| notification-service | Service de notification |
| workitem-service | Service d'élément de travail |

Tableau 1-15. Groupe de catalogues de services (services de gouvernance) (suite)

| Service | Description |
|------------------|-----------------------|
| approval-service | Service d'approbation |
| catalog-service | Catalogue de services |

Tableau 1-16. Groupe de services IaaS

| Service | Description |
|---------------------|----------------------|
| iaas-proxy-provider | Proxy IaaS |
| iaas-server | Machine Windows IaaS |

Tableau 1-17. XaaS

| Service | Description |
|---------------------------|---|
| vco | vRealize Orchestrator |
| advanced-designer-service | Blueprints XaaS et actions de ressource |

Utilisation de la journalisation d'audit de vRealize Automation

vRealize Automation propose la journalisation d'audit pour prendre en charge la collecte et la rétention des événements système importants.

Actuellement, vRealize Automation prend en charge la journalisation d'audit en tant qu'extension de la journalisation des événements. Cette fonctionnalité fournit des informations d'audit base. Les paramètres de rétention ne sont configurables qu'en utilisant les appels du service broker d'événements de l'instance de REST API de vRealize Automation. La journalisation d'audit est actuellement accessible par les administrateurs de locataire et les administrateurs système qui peuvent se connecter aux locataires. Elle fournit des capacités de recherche et de filtrage d'événements.

Par défaut, vRealize Automation prend en charge la journalisation d'audit pour l'abonnement aux workflows, les points de terminaison et la création, mise à jour et suppressions d'événements par le groupe fabric. vRealize Automation prend également en charge la personnalisation de la journalisation d'audit pour divers événements IaaS.

La journalisation d'audit de vRealize Automation est désactivée par défaut. Vous pouvez l'activer ou la désactiver en cochant ou en décochant la case **Activé** de la section Intégration du journal d'audit sur la page **vRA > Journaux** de l'interface de gestion de dispositif virtuel.

Les informations des journaux d'audit s'affichent sur la page Journaux des événements standard. En tant qu'administrateur de locataire, sélectionnez **Administration > Journaux des événements** pour afficher cette page. Les événements d'audit sont identifiés dans le champ tableau du journal des événements par la désignation Audit dans le champ Type d'événement. Chaque entrée fournit une description pour chaque événement et indique le locataire, l'heure, l'utilisateur et le nom du service associé.

L'activation de la journalisation d'audit pour tous les autres événements IaaS nécessite un fichier de configuration personnalisé et l'exécution des commandes appropriées sur votre machine hôte IaaS. Contactez les services professionnels de VMware pour obtenir une assistance.

Vous pouvez configurer vRealize Automation pour exporter les événements vers un serveur syslog externe, notamment VMware Log Insight.

Configurer vRealize Automation pour la journalisation d'audit de Log Insight

Vous pouvez configurer vRealize Automation pour exporter les événements d'audit vers VMware Log Insight afin de faciliter l'affichage des événements d'audit.

La journalisation d'audit est désactivée par défaut et vous devez l'activer pour générer et afficher les événements de journalisation d'audit.

S'il est utilisé, SSL est configuré sur dispositif vRealize Automation où se trouve l'agent Log Insight, et il s'agit de la connexion au serveur Log Insight Syslog. Pour utiliser SSL, vous devez configurer les certificats appropriés et la connectivité entre vRealize Automation et le serveur Log Insight installé sur votre déploiement.

Conditions préalables

vRealize Automation utilise l'agent Log Insight qui est installé par défaut sur un déploiement vRealize Automation pour lire les entrées de journal et les afficher dans Log Insight.

Procédure

- 1 Connectez-vous à l'interface de gestion de dispositifs virtuels en tant qu'administrateur système.
- 2 Sélectionnez **vRA > Journaux**.
- 3 Vérifiez que la case à cocher **Activé** pour la journalisation d'audit est activée sous l'en-tête Intégration de journal d'audit.
- 4 Entrez le nom de la machine **Hôte** pour le serveur Log Insight sous l'en-tête Configuration de l'agent Log Insight.
 - a Entrez le nom de la machine **Hôte** pour l'agent Log Insight.
 - b Entrez le **Port** à utiliser pour la communication avec l'agent Log Insight.
 - c Sélectionnez le protocole de communication.
 - d Utilisez la case à cocher **SSL activé** pour indiquer si SSL doit être utilisé pour la communication entre l'agent Log Insight et le serveur.

Si vous ne souhaitez pas utiliser SSL, vous pouvez ignorer le reste des paramètres sur la page. Si SSL est utilisé, vous devez configurer ces paramètres.

- 5 Effectuez les sélections appropriées dans la section Certificats racine de confiance SSL si vous utilisez SSL.

Par défaut, le dispositif vRealize Automation utilise un certificat auto-signé. Si vous souhaitez utiliser un certificat racine de confiance, vous devez l'importer.

- a Cochez la case appropriée pour indiquer si vous souhaitez utiliser un nouveau certificat ou un certificat existant.

Consultez les notes de la page Configurer la journalisation vRealize Automation de l'interface VAMI pour plus d'informations.

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

- 7 Effectuez les sélections appropriées dans la section Certificats de serveur SSL.

- 8 Utilisez la section Configuration du comportement de l'agent pour configurer l'utilisation des fichiers journaux par l'agent.

Résultats

Les événements de journaux d'audit vRealize Automation sont visibles dans l'interface de Log Insight.

Affichage des informations sur l'hôte pour les clusters dans des déploiements distribués

Vous pouvez collecter des journaux pour tous les nœuds qui sont en cluster dans un déploiement distribué depuis la console de gestion du dispositif vRealize Automation.

Vous pouvez également afficher des informations pour chaque hôte de votre déploiement.

L'onglet **Cluster** de la console de gestion vRealize Automation inclut un tableau Informations sur le déploiement distribué qui affiche les informations suivantes :

- Une liste de tous les nœuds de votre déploiement
- Le nom d'hôte du nœud. Le nom d'hôte est attribué en tant que nom de domaine complet.
- Le délai écoulé depuis la dernière réponse de l'hôte à la console de gestion. Les nœuds des composants IaaS indiquent leur disponibilité toutes les trois minutes et les nœuds des dispositifs virtuels l'indiquent toutes les neuf minutes.
- Le type de composant vRealize Automation. Indique si le nœud est un dispositif virtuel ou un serveur IaaS.

Figure 1-1. tableau Informations sur le déploiement distribué

| | Host / Node Name | Version | Last Connected | Type | State* | Valid* |
|---|------------------------------|-------------|----------------|--------|--------|---------------------------------------|
| ▶ | cava-n-80-175.eng.vmware.com | 7.5.0.378 | 7 minutes ago | MASTER | Up | <input type="button" value="Delete"/> |
| ▶ | cava-n-85-043.eng.vmware.com | 7.5.0.14528 | 14 seconds ago | IAAS | | <input type="button" value="Delete"/> |

Vous pouvez utiliser ce tableau pour surveiller l'activité de votre déploiement. Par exemple, si la colonne Dernière connexion indique qu'un hôte ne s'est pas connecté récemment, cela peut être indicateur d'un problème avec le serveur de l'hôte.

Collecte des journaux

Vous pouvez créer un fichier zip qui contient les fichiers journaux pour tous les hôtes dans votre déploiement en utilisant le bouton Créer un bundle de support sur la page **vRA > Journaux**. Pour plus d'informations, reportez-vous à [Collecter les journaux pour les clusters et les déploiements distribués](#).

Suppression des nœuds du tableau

Lorsque vous supprimez un hôte de votre déploiement, supprimez le nœud correspondant du tableau Informations sur le déploiement distribué pour optimiser les délais de collecte de journaux. Cliquez sur le bouton **Supprimer** pour supprimer un nœud à partir du tableau.

Collecter les journaux pour les clusters et les déploiements distribués

Pour prendre en charge des activités de tenue des registres et de dépannage, vous pouvez créer un fichier zip qui inclut tous les fichiers journaux pour les serveurs dans votre déploiement.

Le tableau Informations sur le déploiement distribué dans l'onglet Cluster de l'Interface de gestion de dispositif virtuel répertorie les nœuds pour lesquels les fichiers journaux sont collectés. Vous pouvez également supprimer des nœuds à partir de ce tableau.

Pour plus d'informations sur la configuration du déploiement du dispositif vRealize Automation, reportez-vous à *Installation de vRealize Automation*.

Procédure

- 1 Connectez-vous à l'interface de gestion de dispositifs virtuels en tant qu'administrateur système.
- 2 Cliquez sur **vRA > Journaux**.
- 3 Cliquez sur **Créer un bundle de support**.

Les fichiers journaux de chaque nœud sont collectés et copiés dans un fichier zip.

Supprimer un nœud du tableau Informations sur le déploiement distribué

Supprimez un nœud lorsque vous souhaitez l'enlever de votre cluster de déploiement ou lorsque vous remplacez un certificat de l'agent de gestion.

Le tableau informations sur le déploiement distribué dans l'onglet Cluster de l'Interface de gestion du dispositif virtuel répertorie les nœuds du cluster applicables. Vous pouvez cliquer sur le bouton **Supprimer** pour n'importe quel nœud du tableau afin de supprimer ce nœud du cluster, ou vous pouvez procéder comme suit.

Procédure

- 1 Connectez-vous au dispositif vRealize Automation avec le nom d'utilisateur **root** et le mot de passe que vous avez spécifié au moment du déploiement du dispositif.

- 2 Cliquez sur l'onglet **Cluster**.

Le tableau des informations sur le déploiement distribué affiche la liste des nœuds pour le déploiement distribué.

- 3 Recherchez l'ID de nœud du nœud à supprimer en ouvrant une invite de commande et en exécutant la commande suivante :

```
/usr/sbin/vcac-config cluster-config-node --action list
```

- 4 Recherchez l'ID du nœud, par exemple `cafe.node.46686239.17144`, dans la sortie JSON.

- 5 Ouvrez une invite de commande et saisissez une commande au format suivant, à l'aide de l'ID de nœud que vous avez obtenu à l'étape précédente.

```
/usr/sbin/vcac-config cluster-config-node  
--action delete --id node-UID
```

Par exemple, entrez la commande suivante pour l'exemple d'ID de nœud `cafe.node.46686239.17144` :

```
/usr/sbin/vcac-config cluster-config-node --action delete --id cafe.node.46686239.17144
```

- 6 Cliquez sur **Actualiser**.

Le nœud ne s'affiche plus à l'écran.

Surveillance de la santé de vRealize Automation

Le service de santé de vRealize Automation évalue la santé fonctionnelle d'un environnement vRealize Automation.

Les administrateurs IaaS configurent le service de santé pour exécuter des suites de tests qui déterminent si les composants sont enregistrés et si les ressources nécessaires sont disponibles. Ce tableau présente les suites de tests fournies par le service de santé et fournit des exemples de tests dans chaque suite.

| Suites de tests du service de santé | Exemples de test |
|---|---|
| Tests système de vRealize Automation | <ul style="list-style-type: none"> ■ Test de connexion VA SSO/identité ■ Vérification de la licence vRealize Automation - La licence a-t-elle expiré ? ■ Vérification du mot de passe racine du dispositif virtuel vRealize Automation - Le mot de passe expire-t-il bientôt ? |
| Tests de locataire de vRealize Automation | <ul style="list-style-type: none"> ■ Vérifier les chemins de stockage des réservations de vSphere ■ Vérifier la stratégie de réservation des affectations de réservations ■ Vérifiez l'état du service de portail |
| Tests pour vRealize Orchestrator | <ul style="list-style-type: none"> ■ Vérifier le nombre de nœuds vRO actifs ■ Vérifier l'utilisation du segment de mémoire java dans les nœuds vRO ■ Vérifier l'état du service vro-server dans les nœuds vRO |

Une fois que vous avez exécuté une suite de tests sur une machine virtuelle, le service de santé indique le nombre de tests ayant réussi ou échoué. Pour chaque test ayant échoué, le service de santé fournit ces liens :

| Lien | Contenu |
|------------|--|
| Cause | Explication de la raison de l'échec du test. |
| Correction | Informations que vous pouvez utiliser pour résoudre le problème. |

Vous pouvez configurer le service de santé pour exécuter des tests de manière planifiée ou uniquement à la demande.

Vous pouvez également utiliser Python pour créer des tests personnalisés. Consultez le document *Guide d'extensibilité du service de santé vRealize Automation*.

Les administrateurs de locataire avec un rôle de consommateur de santé peuvent afficher les résultats du test pour leur location mais ne peuvent pas configurer ou exécuter un test.

Configurez les tests système de vRealize Automation

Un **Administrateur IaaS** configure le service de santé pour exécuter des tests système sur un dispositif virtuel vRealize Automation sélectionné. Ces tests déterminent si les composants, tels que la licence vRealize Automation, sont enregistrés et si les ressources nécessaires, telles que la mémoire, sont disponibles sur le dispositif virtuel. Lorsque vous configurez les tests système, la page Santé affiche les tests sous la forme d'une carte de test.

Pour configurer le service de santé afin d'exécuter des tests système pour vRealize Automation, procédez comme suit.

Conditions préalables

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

Procédure

- 1 Sélectionnez **Administration > Santé**.
- 2 Cliquez sur **Nouvelle configuration**.
- 3 Sur la page Détails de la configuration, fournissez les renseignements demandés.

| Option | Description |
|-------------|--|
| Nom | Votre titre pour cette configuration. Ce titre s'affiche sur la carte de test. |
| Description | Description de la suite de tests. |
| Produit | Sélectionnez vRealize Automation. |
| Planifier | Sélectionnez la fréquence d'exécution de la suite de tests. |

- 4 Cliquez sur **Suivant**.
- 5 Sur la page Sélectionner des suites de tests, sélectionnez **Tests système de vRealize Automation**.
- 6 Cliquez sur **Suivant**.
- 7 Sur la page Configurer les paramètres, fournissez les renseignements demandés.

Tableau 1-18. 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 racine. |

Tableau 1-19. Locataire système vRealize Automation

| Option | Description |
|-------------------------------------|-----------------------------------|
| Administrateur du locataire système | administrateur |
| Mot de passe du locataire système | Mot de passe de l'administrateur. |

Tableau 1-20. Surveillance de l'espace disque vRealize Automation

| Option | Description |
|--------------------------------------|---|
| Pourcentage du seuil d'avertissement | Pourcentage acceptable d'espace disque du dispositif virtuel qui est utilisé avant l'échec du test d'avertissement. |
| Pourcentage de seuil critique | Pourcentage acceptable d'espace disque du dispositif virtuel qui est utilisé avant l'échec du test critique. |

- 8 Cliquez sur **Suivant**.
- 9 Sur la page Résumé, vérifiez les informations.
- 10 Cliquez sur **Terminer**.

Tests exécutés conformément à la planification sélectionnée.

Étape suivante

[Afficher les résultats de la suite de tests du service de santé vRealize Automation](#)

Configurez les tests de locataire de vRealize Automation

Un **administrateur IaaS** configure le service de santé pour exécuter des tests de locataire sur un dispositif virtuel vRealize Automation sélectionné. Ces tests déterminent si les composants liés au locataire, tels que des services logiciels, sont enregistrés et si les ressources nécessaires, telles que des machines virtuelles vSphere, sont disponibles sur le dispositif virtuel. Lorsque vous configurez les tests de locataire, la page Santé affiche les tests sous la forme d'une carte de test.

Pour configurer le service de santé pour exécuter des tests de locataire pour vRealize Automation, procédez comme suit.

Conditions préalables

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

Procédure

- 1 Sélectionnez **Administration > Santé**.
- 2 Cliquez sur **Nouvelle configuration**.

- 3 Sur la page Détails de la configuration, fournissez les renseignements demandés.

| Option | Description |
|-------------|--|
| Nom | Votre titre pour cette configuration. Ce titre s'affiche sur la carte de test. |
| Description | Description des tests. |
| Produit | Sélectionnez vRealize Automation. |
| Planifier | Sélectionnez la fréquence d'exécution de ces tests. |

- 4 Cliquez sur **Suivant**.
- 5 Sur la page Sélectionner les suites de tests, sélectionnez **Tests de locataire pour vRealize Automation**.
- 6 Cliquez sur **Suivant**.
- 7 Sur la page Configurer les paramètres, fournissez les renseignements demandés.

Tableau 1-21. Dispositif virtuel vRealize Automation

| Option | Description |
|--|--|
| Adresse Web vRealize Automation | <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 de l'hôte SSH. Par exemple, <code>ssh-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) | Période maximale en millisecondes pendant laquelle le système attend une réponse. |

Tableau 1-22. Locataire vRealize Automation

| Option | Description |
|---|--|
| Locataire en cours de test | qe |
| Nom d'utilisateur administrateur Fabric | Nom d'utilisateur administrateur Fabric. 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. |

Tableau 1-23. Locataire système vRealize Automation

| Option | Description |
|-------------------------------------|-----------------------------------|
| Administrateur du locataire système | administrateur |
| Mot de passe du locataire système | Mot de passe de l'administrateur. |

Tableau 1-24. Surveillance de l'espace disque vRealize Automation

| Option | Description |
|-------------------------------|--|
| Pourcentage de seuil critique | Pourcentage acceptable d'espace disque du dispositif virtuel qui est utilisé avant l'échec du test critique. |

- 8 Cliquez sur **Suivant**.
- 9 Sur la page Résumé, vérifiez les informations.
- 10 Cliquez sur **Terminer**.

Tests exécutés conformément à la planification sélectionnée.

Étape suivante

[Afficher les résultats de la suite de tests du service de santé vRealize Automation](#)

Configuration des tests pour vRealize Orchestrator

Un **administrateur IaaS** configure le service de santé pour exécuter des tests pour vRealize Orchestrator sur l'hôte vRealize Orchestrator. Ces tests confirment que les composants, tels que le service vro-server, sont enregistrés et que les ressources nécessaires, telles qu'un segment de mémoire Java suffisant, sont disponibles sur la machine hôte. Lorsque vous configurez les tests vRealize Orchestrator, la page Santé affiche les tests sous la forme d'une carte de test.

Conditions préalables

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

Procédure

- 1 Sélectionnez **Administration > Santé**.
- 2 Cliquez sur **Nouvelle configuration**.
- 3 Sur la page Détails de la configuration, fournissez les renseignements demandés.

| Option | Description |
|-------------|--|
| Nom | Votre titre pour cette configuration. Ce titre s'affiche sur la carte de test. |
| Description | Description des tests. |

| Option | Description |
|-----------|--|
| Produit | Sélectionnez vRealize Orchestrator. |
| Planifier | Sélectionnez la fréquence d'exécution des tests. |

- 4 Cliquez sur **Suivant**.
- 5 Sur la page Sélectionner les suites de tests, sélectionnez les **Tests pour vRealize Orchestrator**.
- 6 Cliquez sur **Suivant**.
- 7 Sur la page Configurer les paramètres, fournissez les renseignements demandés.

Tableau 1-25. Hôte/équilibre de charge vRealize Orchestrator

| Option | Description |
|---|--|
| Adresse du client | <ul style="list-style-type: none"> ■ Pour un déploiement minimal, le nom de domaine complet de l'hôte vRealize Orchestrator. Par exemple, <i>vro-host.domain</i>. ■ Pour un déploiement haute disponibilité, l'URL de base de l'équilibre de charge vRealize Orchestrator, à savoir <i>https://load-balancer-host.domain/</i>. |
| Nom d'utilisateur du client | administrateur |
| Mot de passe du client | Mot de passe de l'administrateur. |
| Nom d'utilisateur de la console SSH | root |
| Mot de passe de la console SSH | Mot de passe racine. |
| Seuil d'utilisation du segment de mémoire | Pourcentage d'espace de segment de mémoire qui est utilisé avant l'échec du test d'avertissement. |

Tableau 1-26. Instances vRealize Orchestrator derrière l'équilibre de charge

| Option | Description |
|-------------------------------------|---|
| Adresse de la console SSH | Adresse IP ou URL de l'instance vRealize Orchestrator derrière l'équilibre de charge. |
| Nom d'utilisateur de la console SSH | Nom de l'utilisateur ayant accès à cette instance. |
| Mot de passe de la console SSH | Mot de passe du nom d'utilisateur. |

- Cliquez sur **AJOUTER** pour ajouter une autre instance vRealize Orchestrator à la liste.
- Cliquez sur **SUPPRIMER** pour supprimer une instance vRealize Orchestrator sélectionnée dans la liste des instances derrière l'équilibre de charge.

- 8 Cliquez sur **Suivant**.
- 9 Sur la page Résumé, vérifiez les informations.

10 Cliquez sur **Terminer**.

Tests exécutés conformément à la planification sélectionnée.

Étape suivante

[Afficher les résultats de la suite de tests du service de santé vRealize Automation](#)

Suite de tests personnalisés

Vous pouvez utiliser Python afin de créer une suite de tests personnalisés pour le service de santé vRealize Automation.

La création d'une suite de tests personnalisés vous permet d'étendre les tests fournis pour le service de santé en ajoutant une suite de tests pour déterminer la santé de composants vRealize Automation supplémentaires. Pour plus d'informations sur la création d'une suite de tests personnalisés, consultez le document *Guide d'extensibilité du service de santé vRealize Automation*.

Ajouter une suite de tests personnalisés

Un **administrateur IaaS** doit ajouter une suite de tests personnalisés au service de santé vRealize Automation avant de procéder à la suite de tests.

Pour ajouter une suite de tests personnalisés pour une ressource vRealize Automation, procédez comme suit.

Conditions préalables

- Créer une roue Python pour les fichiers de suites de tests personnalisés. Pour plus d'informations, consultez le *Guide d'extensibilité vRealize Automation du service de santé*.
- Connectez-vous à vRealize Automation en tant qu'**administrateur IaaS**.

Procédure

- 1** Cliquez sur **Administration > Santé**.
- 2** Dans le coin supérieur droit, cliquez sur l'icône d'engrenage et sélectionnez **Extensibilité**.
- 3** Cliquez sur **Nouvelle ressource**.
- 4** Dans la boîte de dialogue Ajouter une ressource, fournissez les renseignements demandés.

| Option | Description |
|-----------------------------|---|
| Titre de la ressource | Nom et numéro de version de la suite de tests en cours d'exécution, par exemple, Infoblox 1.0. |
| Description de la ressource | Description des tests contenus dans la roue Python. |
| Version de la ressource | Numéro de version de la suite de tests. |
| Fichier de la ressource | Cliquez sur Choisir un fichier et sélectionnez le fichier de suite de tests personnalisés. |

5 Cliquez sur **Ajouter**.

Une nouvelle ligne est ajoutée au tableau de ressources avec l'état TÉLÉCHARGÉ. Lorsque l'état passe à INSTALLÉ, votre suite de tests est prête à être utilisée. Si le processus d'installation échoue, une fenêtre contextuelle indique un motif.

Note Si la page ne s'actualise pas, cliquez sur l'icône d'actualisation.

Étape suivante

[Exécuter une suite de tests personnalisés.](#)

Exécuter une suite de tests personnalisés

Un **administrateur laaS** configure le service de santé pour exécuter une suite de tests personnalisés dans l'environnement vRealize Automation. Lorsque vous configurez la suite de tests personnalisés, la page Santé affiche la suite de tests sous la forme d'une carte de test.

Pour configurer le service de santé pour exécuter une suite de tests personnalisés pour vRealize Automation, procédez comme suit.

Conditions préalables

- [Ajouter une suite de tests personnalisés.](#)
- Connectez-vous à vRealize Automation en tant qu'**administrateur laaS**.

Procédure

- 1 Sélectionnez **Administration > Santé**.
- 2 Cliquez sur **Nouvelle configuration**.
- 3 Sur la page Détails de la configuration, fournissez les renseignements demandés.

| Option | Description |
|-------------|---|
| Nom | Votre titre pour cette configuration. Ce titre s'affiche sur la carte de test. |
| Description | Description de la suite de tests. |
| Produit | Sélectionnez le produit que vous souhaitez tester dans le menu déroulant Produit . |
| Planifier | Sélectionnez la fréquence d'exécution de cette suite de tests. |

- 4 Cliquez sur **Suivant**.
- 5 Sur la page Sélectionner les suites de tests, sélectionnez la suite de tests personnalisée, puis cliquez sur **Suivant**.
- 6 Sur la page Configurer les paramètres, entrez les informations demandées, puis cliquez sur **Suivant**.

- 7 Sur la page Résumé, passez en revue les informations, puis cliquez sur **Terminer**.

La suite de tests personnalisés est exécutée en fonction de la planification sélectionnée.

Étape suivante

[Afficher les résultats de la suite de tests du service de santé vRealize Automation](#)

Afficher les résultats de la suite de tests du service de santé vRealize Automation

Vous pouvez afficher les résultats du test du service de santé après l'exécution des tests.

La page Santé affiche chaque suite de tests configurée comme une carte de test. Lorsqu'une suite de tests s'exécute, le résultat s'affiche au milieu de la carte de test.

Les cartes de test qui s'affichent sur la page Santé sont filtrées en fonction de vos privilèges.

- Les administrateurs IaaS peuvent voir toutes les cartes de test.
- Les administrateurs de locataire avec le rôle de consommateur de santé peuvent voir uniquement la carte de test de leur locataire.

Conditions préalables

- La suite de tests configurée a été exécutée selon la planification définie.
- Connectez-vous à la console vRealize Automation en tant qu'**administrateur IaaS** ou en tant qu'**administrateur de locataire**.

Procédure

- 1 Sélectionnez **Administration > Santé**.
- 2 Si l'exécution d'un test n'est pas planifiée, cliquez sur **Exécuter** sur la carte de test.
- 3 Une fois les tests terminés, cliquez sur le centre d'une carte de test.

Une page affiche l'état de chaque test. Pour voir la raison pour laquelle un test a échoué, cliquez sur **Cause**. Pour ouvrir une rubrique qui explique comment résoudre le problème, cliquez sur le lien **Correction** s'il est disponible.

Dépannage du service de santé

Les rubriques de dépannage du service de santé proposent des solutions aux problèmes que vous pouvez rencontrer lorsque vous utilisez le service de santé.

Échec de test de l'état du service

Vous pouvez corriger un test de service ayant échoué en modifiant le paramètre de planification du test.

Problème

Si un test de l'état du service échoue et que vous cliquez sur **Cause**, le message suivant s'affiche : Impossible d'établir une connexion SSH ; message d'exception : [Échec de l'authentification].

Cause

Lorsque la suite de tests est planifiée pour s'exécuter toutes les 15 minutes, la connexion système verrouille le compte d'utilisateur racine.

Solution

- ◆ Modifiez la planification du test sur **Aucun**, patientez 15 minutes et réexécutez la suite de tests.

Après la mise à niveau, la page Santé dans la console du dispositif est vide

Après la mise à niveau de vRealize Automation, la page Santé dans la console du dispositif est vide.

Problème

Le service de santé ne démarre pas après la mise à niveau.

Solution

- ◆ Sur chaque dispositif virtuel vRealize Automation, ouvrez une invite de commande en tant qu'utilisateur **root** et exécutez les commandes suivantes.
 - a Pour configurer le démarrage automatique du service de santé, exécutez cette commande.

```
chkconfig vrhb-service on
```
 - b Pour démarrer le service de santé sur ce dispositif virtuel, exécutez cette commande.

```
service vrhb-service start
```

Surveillance des ressources d'environnement vRealize Automation à l'aide de SNMP

En tant qu'administrateur système connaissant le protocole SNMP, vous souhaitez utiliser vRealize Automation REST API pour vSNMP afin de faciliter la surveillance de vos nœuds vRealize Automation. vSNMP vous permet d'utiliser SNMP en tant que système d'avertissement précoce chiffré lorsque vRealize Automation est sur le point de manquer de CPU, de RAM et d'espace disque afin d'éviter les ralentissements.

Vous pouvez surveiller manuellement les OID SNMP ou vous pouvez surveiller activement les ressources en définissant des interruptions SNMP.

Par exemple, si vSNMP vous envoie un événement « Utilisation élevée du CPU détectée », vous pouvez commencer à collecter des informations sur les processus consommant le CPU et déterminer celui qui utilise des ressources excessives. Vous pouvez ensuite mettre en corrélation le CPU, la mémoire et d'autres utilisations pour résoudre des problèmes supplémentaires.

vRealize Automation vSNMP vous permet d'afficher l'intégralité de l'arborescence Linux afin de surveiller et récupérer des données à l'aide de REST API, ou à l'aide du démon vSNMPD exécuté sur les instances de vRealize Automation.

vRealize Automation SNMP ne dispose pas d'une interface d'utilisation générale. Vous devez utiliser les commandes de REST API ou du démon.

Pour plus d'informations, reportez-vous à la section « Utilisation de SNMP pour surveiller vRealize Automation » du Guide de programmation de vRealize Automation. Pour obtenir le Guide de programmation, reportez-vous à la page [Documentation de l'API de vRealize Automation](#) et sélectionnez le lien correspondant à votre version.

Surveillance et gestion des ressources

Différents rôles de vRealize Automation permettent de surveiller l'utilisation des ressources et de gérer l'infrastructure de différentes manières.

Choisir un scénario de surveillance des ressources

Les administrateurs Fabric, les administrateurs de locataire et les gestionnaires de groupes d'activité font face à des problèmes différents en matière de surveillance des ressources. C'est pour cette raison que vRealize Automation vous permet de surveiller différentes facettes de l'utilisation des ressources.

Par exemple, un administrateur Fabric s'intéresse à la surveillance de la consommation des ressources des réservation et des ressources de calcul, alors qu'un administrateur de locataire s'intéresse davantage à l'utilisation des ressources des groupes de provisionnement au sein d'un locataire. En fonction de votre rôle et de l'utilisation spécifique des ressources que vous surveillez, vRealize Automation vous offre différentes manières de suivre la consommation des ressources.

Tableau 1-27. Choisir un scénario de surveillance des ressources

| Scénario de surveillance des ressources | Privilèges requis | Emplacement |
|---|--|--|
| Surveiller le volume de stockage physique et de mémoire de vos ressources de calcul qui est actuellement consommé et déterminez la capacité disponible restante. Vous pouvez également surveiller le nombre de machines réservées et attribuées provisionnées sur chaque ressource de calcul. | Administrateur Fabric (surveiller l'utilisation des ressources sur les ressources de calcul de votre groupe Fabric) | Infrastructure > Ressources de calcul > Ressources de calcul |
| Surveiller les machines qui sont actuellement provisionnées et gérées par vRealize Automation. | Administrateur Fabric | Infrastructure > Machines > Machines gérées |
| Surveiller le volume de stockage, de mémoire et le quota de machine de votre réservation qui est actuellement attribué et déterminez la capacité disponible à la réservation. | Administrateur Fabric (surveiller l'utilisation des ressources pour les réservations sur vos ressources de calcul et machines physiques) | Infrastructure > Réservations > Réservations. |
| Surveiller le volume de stockage, de mémoire et le quota de machine que vos groupes d'activité utilisent actuellement et déterminez la capacité qui leur reste sur la réserve. | <ul style="list-style-type: none"> ■ Administrateur de locataire (surveiller l'utilisation des ressources pour tous les groupes de votre locataire) ■ Gestionnaire de groupes d'activité (surveiller l'utilisation des ressources pour les groupes que vous gérez) | Administration > Utilisateurs et groupes > Groupes d'activité |

Terminologie de l'utilisation des ressources

vRealize Automation utilise une terminologie explicite pour faire la distinction entre des ressources disponibles, des ressources mises à l'écart pour des utilisations spécifiques et des ressources consommées activement par des machines provisionnées.

Le tableau Terminologie de l'utilisation des ressources explique la terminologie qu'utilise vRealize Automation pour afficher l'utilisation des ressources.

Tableau 1-28. Terminologie de l'utilisation des ressources

| Terme | Description |
|-----------------|---|
| Physique | Indique la capacité de mémoire ou de stockage actuelle d'une ressource de calcul. |
| Réservé | Indique le quota et la capacité de mémoire et de stockage de la machine mis à l'écart pour une réservation. Par exemple, si une ressource de calcul a une capacité physique de 600 Go et qu'il y a trois réservations dessus de 100 Go chacune, le stockage réservé de la ressource de calcul est de 300 Go et le stockage réservé est de 50 %. |
| Géré | Indique que la machine est provisionnée et actuellement gérée par vRealize Automation. |

Tableau 1-28. Terminologie de l'utilisation des ressources (suite)

| Terme | Description |
|-------------------|---|
| Alloué | Indique le quota, la mémoire ou les ressources de stockage de la machine activement consommées par des machines provisionnées. Par exemple, prenons une réservation avec un quota de machine de 10. Si elle contient 15 machines provisionnées, mais que seules 6 d'entre elles sont actuellement sous tension, le quota de la machine est alloué à 60 pour cent. |
| Utilisé | La valeur de la colonne Utilisé est toujours égale à la valeur de la colonne Alloué . |
| Disponible | Indique la capacité physique non utilisée d'un chemin de stockage. |

Connexion à une machine de cloud

La première fois que vous vous connectez à une machine de cloud, vous devez vous connecter en tant qu'administrateur.

Vous pouvez ensuite ajouter des informations d'identification avec lesquelles vous vous connectez à la console vRealize Automation en tant qu'utilisateur de la machine et vous connecter avec vos informations d'identification vRealize Automation dès à présent.

Important Si vous utilisez Amazon Web Services, RDP ou SSH doit être activé sur l'instance des machines Amazon et ces machines doivent être incluses dans un groupe de sécurité dans lequel les ports adéquats sont ouverts.

Collecter des informations d'identification utilisateur pour une machine Amazon

Pour vous connecter à une machine Amazon en tant qu'administrateur, il vous faut découvrir le mot de passe de l'administrateur de la machine.

Le mot de passe d'administrateur est disponible sur la page de détails des informations de la machine. Si l'image de la machine Amazon à partir de laquelle la machine a été provisionnée n'est pas configurée pour générer le mot de passe de l'administrateur à chaque démarrage, vous devez trouver le mot de passe au moyen d'une autre technique. Pour des informations à ce sujet, faites une recherche parmi les rubriques *Connect to Your Amazon EC2 Instance* dans la documentation Amazon.

Si nécessaire, vous pouvez créer les informations d'identification utilisateur vRealize Automation requises. Les informations d'identification utilisateur sont ensuite valides pour des connexions ultérieures à cette machine.

Conditions préalables

- La machine Amazon a déjà été provisionnée.
- Connectez-vous à vRealize Automation en tant que propriétaire de la machine, **gestionnaire de groupes d'activité** ou **utilisateur de support technique**.
- La connexion via RDP ou SSH est activée sur l'image de la machine Amazon qui sera utilisée pour le provisionnement.

- Les machines appartiennent à un groupe de sécurité dans lesquels les bons ports sont ouverts.

Procédure

1 Accédez à la page **Éléments** et filtrez les groupes que vous gérez ou un groupe spécifique.

2 Sélectionnez la machine Amazon dans la liste des machines.

Vous pouvez cliquer sur **Afficher les détails** dans le menu déroulant **Actions** pour afficher des détails tels que le type de machine.

3 Sélectionnez **Modifier** dans le menu déroulant **Actions**.

4 Cliquez sur **Afficher le mot de passe administrateur** pour obtenir le mot de passe d'administrateur de la machine.

Vous avez également la possibilité d'obtenir le mot de passe au moyen d'une procédure Amazon externe.

5 Cliquez **Se connecter via RDP** dans le menu déroulant **Actions**.

6 Cliquez sur **Utiliser un autre compte** lorsque vous êtes invité à entrer les informations d'identification pour la connexion.

7 Saisissez **LOCAL\Administrator** lorsque vous êtes invité à entrer le nom d'utilisateur.

8 Saisissez le mot de passe administrateur lorsque vous y êtes invité.

9 Cliquez sur **OK**.

Vous êtes désormais connecté à la machine en tant qu'administrateur.

10 Ajoutez vos informations d'identification vRealize Automation comme approprié. Par exemple, sur une machine serveur Windows, ouvrez le gestionnaire de serveur et sélectionnez **Configuration > Utilisateurs locaux et groupes** et ajoutez vos informations d'identification au format **DOMAINE\nomdutilisateur**, au groupe **Utilisateurs du bureau à distance**.

Votre nom d'utilisateur et votre mot de passe vRealize Automation sont désormais des informations d'identification valides pour des connexions ultérieures à cette machine.

11 Déconnectez-vous de la machine Amazon.

12 Cliquez **Se connecter via RDP** dans le menu déroulant **Actions**.

13 Lorsque vous êtes invités à vous connecter, saisissez votre nom d'utilisateur et votre mot de passe vRealize Automation pour vous connecter à la machine.

Résultats

Les propriétaires de machines peuvent désormais se connecter à la machine avec leurs informations d'identification vRealize Automation.

Collecter des informations d'identification utilisateur pour une machine vCloud

Pour vous connecter à une machine vCloud Air ou vCloud Director en tant qu'administrateur, il vous faut découvrir le mot de passe de l'administrateur de la machine.

Le mot de passe d'administrateur est disponible sur la page de détails des informations de la machine. Si l'image de la machine à partir de laquelle la machine a été provisionnée n'est pas configurée pour générer le mot de passe de l'administrateur à chaque démarrage, vous pouvez trouver le mot de passe au moyen d'une autre technique. Pour obtenir des informations sur une autre manière d'obtenir le mot de passe de l'administrateur, consultez la documentation de vCloud Air ou de vCloud Director.

Si nécessaire, vous pouvez créer les informations d'identification utilisateur vRealize Automation requises. Les informations d'identification utilisateur sont ensuite valides pour des connexions ultérieures à cette machine.

Conditions préalables

- La machine vCloud Air ou vCloud Director a déjà été provisionnée.
- Connectez-vous à vRealize Automation en tant que propriétaire de la machine, **gestionnaire de groupes d'activité** ou **utilisateur de support technique**.
- La connexion via RDP ou SSH est activée sur l'image de la machine vCloud Air ou vCloud Director qui sera utilisée pour le provisionnement.
- Les machines appartiennent à un groupe de sécurité dans lesquels les bons ports sont ouverts.

Procédure

- 1 Accédez à la page **Éléments** et filtrez les groupes que vous gérez ou un groupe spécifique.
- 2 Sélectionnez la machine vCloud Air ou vCloud Director dans la liste des machines.
Vous pouvez cliquer sur **Afficher les détails** dans le menu déroulant **Actions** pour afficher des détails tels que le type de machine.
- 3 Sélectionnez **Modifier** dans le menu déroulant **Actions**.
- 4 Cliquez sur **Afficher le mot de passe administrateur** pour obtenir le mot de passe d'administrateur de la machine.
Vous avez également la possibilité d'obtenir le mot de passe au moyen d'une procédure vCloud Air ou vCloud Director externe.
- 5 Cliquez **Se connecter via RDP** dans le menu déroulant **Actions**.
- 6 Cliquez sur **Utiliser un autre compte** lorsque vous êtes invité à entrer les informations d'identification pour la connexion.
- 7 Saisissez **LOCAL\Administrator** lorsque vous êtes invité à entrer le nom d'utilisateur.
- 8 Saisissez le mot de passe administrateur lorsque vous y êtes invité.

9 Cliquez sur **OK**.

Vous êtes désormais connecté à la machine en tant qu'administrateur.

10 Ajoutez vos informations d'identification vRealize Automation comme approprié. Par exemple, sur une machine serveur Windows, ouvrez le gestionnaire de serveur et sélectionnez **Configuration > Utilisateurs locaux et groupes** et ajoutez vos informations d'identification au format **DOMAINE\nomdutilisateur**, au groupe **Utilisateurs du bureau à distance**.

Votre nom d'utilisateur et votre mot de passe vRealize Automation sont désormais des informations d'identification valides pour des connexions ultérieures à cette machine.

11 Déconnectez-vous de la machine vCloud Air ou vCloud Director.

12 Cliquez **Se connecter via RDP** dans le menu déroulant **Actions**.

13 Lorsque vous êtes invités à vous connecter, saisissez votre nom d'utilisateur et votre mot de passe vRealize Automation pour vous connecter à la machine.

Résultats

Les propriétaires de machines peuvent désormais se connecter à la machine avec leurs informations d'identification vRealize Automation.

Réduction de l'utilisation de la réservation par attrition

Les administrateurs Fabric peuvent réduire le nombre de machines sur une réservation définie à long terme tout en maintenant actives la réservation et les machines existantes provisionnées dessus.

Vous pouvez réduire le quota de la machine réservée, sa mémoire et le stockage d'une réservation virtuelle sous la quantité allouée actuellement. Cela vous permet de continuer de gérer les machines existantes sans effectuer de modification tout en empêchant le provisionnement de nouvelles machines tant la quantité allouée ne passe pas sous le niveau réservé.

Note Du fait que les machines virtuelles mises hors tension ne sont pas incluses dans le total des quotas de mémoire et de machine alloués, la réduction de l'allocation de mémoire ou de machine d'une réservation peut empêcher que les machines actuellement hors tension soit remises sous tension.

Par exemple, prenons un groupe d'activité avec une réservation contenant 20 machines provisionnées définies pour expirer au cours des 90 prochains jours. Si vous souhaitez réduire cette réservation par attrition à 15 machines au maximum, vous pouvez modifier la réservation pour réduire le quota de 20 machines à 15. Aucune autre machine ne pourra être provisionnée dans la réservation tant que le nombre de machines sur celle-ci ne diminuera pas naturellement par les expirations à venir.

Désaffectation d'un chemin de stockage

Si vous désaffectez un chemin de stockage et que vous déplacez les machines vers un nouveau chemin de stockage, un administrateur Fabric doit désactiver le chemin de stockage dans vRealize Automation.

La présentation suivante est une présentation générale de la séquence d'étapes requises pour désaffecter un chemin de stockage :

- 1 Un administrateur Fabric désactive le chemin de stockage sur toutes les réservations qui l'utilisent. Reportez-vous à [Désactiver un chemin de stockage](#).
- 2 Déplacez les machines vers un nouveau chemin de stockage en dehors de vRealize Automation.
- 3 Attendez que vRealize Automation exécute automatiquement la collecte des données d'inventaire ou initialisez la collecte des données d'inventaire manuellement. Reportez-vous à [Configurer la collecte des données de ressources de calcul](#).

Désactiver un chemin de stockage



Les administrateurs Fabric peuvent désactiver les chemins de stockage sur les réservations lorsque des chemins de stockage sont désaffectés.

Note Pour chaque réservation où vous désactivez un chemin de stockage, vérifiez qu'il reste suffisamment d'espace sur les autres chemins de stockage activés.

Conditions préalables

Connectez-vous à vRealize Automation en tant qu'**administrateur Fabric**.

Procédure

- 1 Sélectionnez **Infrastructure > Réservations > Réservations**.
- 2 Pointez sur la réservation sur laquelle le chemin de stockage que vous désaffectez est utilisé et cliquez sur **Modifier**.
- 3 Cliquez sur l'onglet **Ressources**.
- 4 Localisez le chemin de stockage que vous désaffectez.
- 5 Cliquez sur l'icône **Modifier** (.
- 6 Cochez la case dans la colonne Désactivé pour désactiver ce chemin de stockage.
- 7 Cliquez sur l'icône **Enregistrer** (.
- 8 Cliquez sur **OK**.
- 9 Répétez cette procédure pour toutes les réservations qui utilisent le chemin de stockage que vous désaffectez.

Collecte des données

vRealize Automation collecte les données des points de terminaison sources de l'infrastructure et de leurs ressources de calcul.

La collecte de données se produit à intervalles réguliers. Chaque type de collecte de données a un intervalle par défaut que vous pouvez remplacer ou modifier. Chaque type de collecte de données a également un intervalle de délai d'expiration par défaut que vous pouvez remplacer ou modifier.

Les administrateurs IaaS peuvent lancer manuellement la collecte des données des points de terminaison source de l'infrastructure et les administrateurs Fabric peuvent initier manuellement la collecte des données pour les ressources de calcul.

Tableau 1-29. Types de collectes de données

| Type de collecte de données | Description |
|---|--|
| Collecte des données du point de terminaison source de l'infrastructure | <p>Met à jour les informations concernant les hôtes, modèles et images ISO de virtualisation, pour les environnements de virtualisation. Met à jour les centres de données et modèles pour vCloud Director. Met à jour les régions Amazon et les machines provisionnées sur des régions Amazon.</p> <p>La collecte de données de point de terminaison s'exécute toutes les 4 heures.</p> |
| Collecte des données d'inventaire | <p>Met à jour l'enregistrement des machines virtuelles dont l'utilisation de la ressource est liée à une ressource de calcul spécifique, y compris les informations détaillées sur les réseaux, le stockage et les machines virtuelles. Cet enregistrement inclut également des informations sur les machines virtuelles non gérées qui sont des machines provisionnées en dehors de vRealize Automation.</p> <p>La collecte de données d'inventaire s'exécute toutes les 24 heures.</p> <p>L'intervalle de délai d'expiration par défaut pour la collecte de données d'inventaire est 2 heures.</p> |
| Collecte des données d'état | <p>Met à jour l'enregistrement de l'état d'alimentation de chaque machine découverte par le biais de la collecte de données d'inventaire. La collecte des données d'état enregistre les machines manquantes gérées par vRealize Automation mais qui ne peuvent être détectées sur la ressource de calcul de virtualisation ou le point de terminaison cloud.</p> <p>La collecte de données d'état s'exécute toutes les 15 minutes.</p> <p>L'intervalle de délai d'expiration par défaut pour la collecte de données d'état est 1 heure.</p> |

Tableau 1-29. Types de collectes de données (suite)

| Type de collecte de données | Description |
|--|---|
| Collecte de données de performance (ressources de calcul vSphere seulement) | <p>Met à jour l'enregistrement de l'utilisation moyenne de la CPU, du stockage, de la mémoire et du réseau de chaque machine virtuelle découverte par le biais de la collecte de données d'inventaire.</p> <p>La collecte de données de performance s'exécute toutes les 24 heures.</p> <p>L'intervalle de délai d'expiration par défaut pour la collecte de données de performance est 2 heures.</p> |
| Collecte de données d'inventaire de réseau et de sécurité (ressources de calcul vSphere seulement) | <p>Met à jour l'enregistrement des données du réseau et de la sécurité associées à vCloud Networking and Security et à NSX, notamment les informations sur les groupes de sécurité et l'équilibrage de charge de chaque machine à la suite de la collecte des données d'inventaire.</p> |
| Collecte des données WMI (ressources de calcul Windows uniquement) | <p>Met à jour l'enregistrement des données de gestion de chaque machine Windows. Un agent WMI doit être installé, en général sur l'hôte du service gestionnaire, et activé de manière à collecter les données des machines Windows.</p> |

Démarrer la collecte de données de point de terminaison manuellement

La collecte de données de point de terminaison s'exécute automatiquement toutes les 4 heures, mais les administrateurs IaaS peuvent démarrer manuellement la collecte de données de point de terminaison à tout moment pour les points de terminaison ne nécessitant pas d'agents proxy.

La page **Collecte des données** fournit des informations sur l'état et l'âge des collectes de données. Elle vous permet également de démarrer manuellement une nouvelle collecte de données de point de terminaison.

Conditions préalables

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

Procédure

- 1 Sélectionnez **Infrastructure > Points de terminaison > Points de terminaison**.
- 2 Cliquez sur la ligne du point de terminaison dont vous souhaitez collecter des données.
- 3 Sélectionnez une action de collecte de données disponible.

Configurer la collecte des données de ressources de calcul

Vous pouvez activer ou désactiver la collecte de données, configurer la fréquence de collecte de données ou demander manuellement la collecte de données.

La page **Collecte des données** fournit des informations sur l'état et l'âge des collectes des données. Elle vous permet également de configurer la collecte des données pour vos ressources de calcul.

Conditions préalables

Connectez-vous à vRealize Automation en tant qu'**administrateur Fabric**.

Procédure

- 1 Sélectionnez **Infrastructure > Ressources de calcul > Ressources de calcul**.
- 2 Pointez vers la ressource de calcul pour laquelle configurer la collecte des données et cliquez sur **Collecte des données**.
- 3 Configurez les spécifications de la collecte des données **Ressources de calcul**.
 - Sélectionnez **Activé** pour activer la collecte des données.
 - Sélectionnez **Désactivé** pour désactiver la collecte des données.
- 4 Configurez la collecte des données **Inventaire**.
 - Sélectionnez **Activé** pour activer la collecte des données.
 - Sélectionnez **Désactivé** pour désactiver la collecte des données.
 - Entrez un nombre dans la zone de texte **Fréquence** pour configurer l'intervalle de temps (en heures) entre les collectes des données d'inventaire.
 - Cliquez sur **Demander maintenant** pour démarrer manuellement la collecte des données.
- 5 Configurez la collecte des données **État**.
 - Sélectionnez **Activé** pour activer la collecte des données.
 - Sélectionnez **Désactivé** pour désactiver la collecte des données.
 - Entrez un nombre dans la zone de texte **Fréquence** pour configurer l'intervalle de temps (en minutes) entre les collectes des données d'état.
 - Cliquez sur **Demander maintenant** pour démarrer manuellement la collecte des données.
- 6 Configurez la collecte des données **Performance**.

Celle-ci est disponible uniquement pour les intégrations vSphere.

 - Sélectionnez **Activé** pour activer la collecte des données.
 - Sélectionnez **Désactivé** pour désactiver la collecte des données.
 - Entrez un nombre dans la zone de texte **Fréquence** pour configurer l'intervalle de temps (en heures) entre les collectes des données de performance.
 - Cliquez sur **Demander maintenant** pour démarrer manuellement la collecte des données.
- 7 Configurez la collecte des données **Inventaire de snapshot**.

Cette option est disponible pour les ressources de calcul gérées par vRealize Business for Cloud.

 - Sélectionnez **Activé** pour activer la collecte des données.
 - Sélectionnez **Désactivé** pour désactiver la collecte des données.

- Entrez un nombre dans la zone de texte **Fréquence** pour configurer l'intervalle de temps (en heures) entre les collectes des données de snapshot.
- Cliquez sur **Demander maintenant** pour démarrer manuellement la collecte des données.

8 Cliquez sur **OK**.

Mettre à jour les données de coût de toutes les ressources de calcul

Les administrateurs Fabric peuvent mettre à jour les informations de coût de toutes les ressources de calcul gérées par vRealize Business for Cloud.

Conditions préalables

Connectez-vous à vRealize Automation en tant qu'**administrateur Fabric**.

Procédure

- 1 Sélectionnez **Infrastructure > Ressources de calcul > Ressources de calcul**.
- 2 Cliquez sur **Mettre à jour le coût**.
- 3 Cliquez sur **Demander maintenant**.

Résultats

Lorsque la mise à jour du coût est terminée, l'état passe à Réussi.

Présentation de la vérification d'allocation vSwap pour les points de terminaison vCenter Server

Vous pouvez utiliser vSwap pour déterminer l'espace d'échange disponible sur une machine cible. La vérification vSwap se produit lorsque vous créez ou reconfigurez une machine virtuelle à partir de vRealize Automation. La vérification d'allocation vSwap est disponible uniquement pour les points de terminaison vCenter Server.

L'allocation de stockage vRealize Automation vérifie si l'espace disque disponible est suffisant sur la banque de données pour tenir compte des disques de machine virtuelle lors d'une demande de création ou de reconfiguration. Cependant, lorsque la machine est sous tension, si l'espace disque disponible n'est pas suffisant pour créer des fichiers d'échange sur le point de terminaison vCenter Server, la mise sous tension de la machine échoue. Lorsque l'opération de mise sous tension échoue, les personnalisations qui dépendent de cette machine échouent également. La machine peut également être éliminée. En fonction de la taille de la demande, les commentaires indiquant que la machine n'a pas été mise sous tension ou n'a pas été provisionnée ne sont pas immédiatement évidents.

Vous pouvez utiliser la vérification d'allocation vSwap pour surmonter ces limites en vérifiant l'espace d'échange disponible pour le fichier d'échange de taille maximale dans le cadre de la procédure de création et de reconfiguration de vRealize Automation pour les points de terminaison vCenter Server. Pour activer la vérification d'allocation vSwap, définissez la propriété personnalisée `VirtualMachine.Storage.ReserveMemory` sur `True` dans le composant de la machine ou le Blueprint général.

Tenez compte des comportements de vérification d'allocation vSwap suivants :

- Le fichier d'échange se trouve dans la banque de données qui contient la machine virtuelle. Les configurations alternatives de vCenter Server pour localiser des fichiers d'échange sur une banque de données dédiée ou une autre banque de données ne sont pas prises en charge.
- La taille de l'échange est prise en compte lors de la création et de la reconfiguration d'une machine virtuelle. La taille maximale de l'échange est la taille de la mémoire de la machine virtuelle.
- Les valeurs réservées pour les réservations de stockage de vRealize Automation dans un hôte ne doivent pas dépasser la capacité physique de la ressource de calcul.
- Lors de la création d'une réservation, la somme des valeurs réservées ne doit pas dépasser l'espace de stockage disponible.
- Les réservations de mémoire au niveau du pool de ressources ou de l'hôte ou de la machine virtuelle sur vSphere ne sont pas collectées à partir du point de terminaison vSphere et ne sont pas prises en compte lors des calculs sur vRealize Automation.
- vSwap ne valide pas l'espace d'échange qui est disponible lors des opérations de mise sous tension des machines existantes.
- Vous devez ré-exécuter la collecte de données pour capturer toute modification apportée au point de terminaison vSphere par rapport à vSwap.

Suppression de sites géographiques de centres de données

Pour supprimer le site géographique d'un centre de données d'un menu utilisateur, un administrateur système doit supprimer les informations sur le site géographique dans le fichier des sites géographiques et un administrateur Fabric doit supprimer les informations sur le site géographique dans la ressource de calcul.

Par exemple, si vous ajoutez Londres au fichiers des sites géographiques, que vous associez dix ressources de calcul à ce site géographique, puis que vous supprimez Londres du fichier, les ressources de calcul sont toujours associées au site géographique Londres et Londres fait toujours partie de la liste déroulante des sites géographiques de la page Confirmer la demande de machine. Pour supprimer ce site géographique de la liste déroulante, un administrateur Fabric doit modifier la ressource de calcul et réinitialiser le site géographique pour qu'il soit vierge pour toutes les ressources de calcul associées à ce site géographique.

La présentation de niveau supérieur de la procédure requise pour supprimer un site géographique de centre de données est la suivante :

- 1 Un administrateur système supprime les informations sur le site géographique du centre de données du fichier des sites géographiques.
- 2 Un administrateur Fabric supprime toutes les associations de ressources de calcul avec le site géographique en modifiant les sites géographiques de chaque ressource de calcul associée.

Surveillance des conteneurs

Vous pouvez surveiller l'état d'un conteneur que vous créez dans Conteneurs pour vRealize Automation.

Après avoir créé vos conteneurs sur la base d'un modèle, vous pouvez contrôler leur état. En cliquant sur **Détails** sur un conteneur, vous pouvez surveiller la bande passante réseau, l'utilisation de CPU et de mémoire, les journaux et les propriétés de ce conteneur.

Importation, mise à jour ou migration de machines virtuelles en bloc

Vous pouvez utiliser la fonctionnalité Importations en bloc pour importer, mettre à jour ou migrer des machines virtuelles vers vRealize Automation. Importations en bloc simplifie la gestion de plusieurs machines dans plusieurs environnements.

Importations en bloc crée un fichier CSV contenant des données de machine virtuelle telles que la réservation, le chemin de stockage, Blueprint, le propriétaire et toute propriété personnalisée. Vous utilisez le fichier CSV pour importer des machines virtuelles dans votre environnement vRealize Automation. Importations en bloc prend en charge les tâches administratives suivantes :

- Importer une ou plusieurs machines virtuelles non gérées afin qu'elles puissent être gérées dans un environnement vRealize Automation.
- Effectuer une modification globale à une propriété de machine virtuelle, par exemple un chemin d'accès au stockage.
- Migrer une machine virtuelle d'un environnement vRealize Automation à l'autre.

Note Seuls vCloud Director et vSphere sont pris en charge pour l'importation en bloc. Définir le filtre sur un autre type de point de terminaison ne génère pas de données dans le fichier CSV.

Vous pouvez exécuter les commandes de la fonctionnalité Importations en bloc à l'aide de la console vRealize Automation ou de l'interface de ligne de commande CloudUtil. Pour obtenir plus d'informations sur l'utilisation de l'interface de ligne de commande CloudUtil, reportez-vous à la documentation de *Extensibilité du cycle de vie*.

Note L'importation en bloc de machines ne contourne pas les étapes de provisionnement normales. Tous les workflows externes existants déclenchés par le service Event Broker pendant le provisionnement sont exécutés pour les machines importées. Vous pouvez désactiver temporairement les workflows pour les machines importées en effectuant l'une des opérations suivantes :

- Désactivez tous les abonnements au service Event Broker. Si vous désactivez des abonnements, vous devez planifier une interruption de service pour votre cluster vRealize Automation, car l'extensibilité ne sera pas appliquée à une machine normale provisionnée pendant ce temps.
 - Ajoutez une condition aux abonnements d'événements à ne pas déclencher lorsqu'une machine est importée. Pour ajouter cette condition, accédez à Abonnements aux événements, sélectionnez l'abonnement à désactiver et ajoutez une propriété personnalisée `VirtualMachine.Imported.ConvergedBlueprint n'est pas égal à <ID du Blueprint importé>`. Cette condition n'a pas d'incidence sur les machines provisionnées normalement et ne s'applique qu'aux machines importées.
-

Conditions préalables

- Connectez-vous à vRealize Automation en tant qu'**administrateur Fabric** et en tant que **gestionnaire de groupes d'activité**.
- Si vous importez des machines virtuelles qui utilisent des adresses IP statiques, préparez un pool d'adresses correctement configuré.

Importer une machine virtuelle dans un environnement vRealize Automation

Vous pouvez importer une machine virtuelle non gérée vers un environnement vRealize Automation.

Une machine virtuelle non gérée existe dans un hyperviseur mais n'est pas gérée dans un environnement vRealize Automation et ne peut pas être consultée sur la console. Une fois que vous avez importé une machine virtuelle non gérée, celle-ci est gérée à l'aide de l'interface de gestion de vRealize Automation. Selon les privilèges dont vous disposez, la machine virtuelle s'affiche dans l'onglet **Machines gérées** ou **Déploiements**.

L'option d'importation en bloc ne prend pas en charge les déploiements qui sont provisionnés à partir d'un Blueprint contenant un réseau NSX et des composants de sécurité ou un composant logiciel.

Conditions préalables

- Connectez-vous à vRealize Automation en tant qu'**administrateur Fabric** et en tant que **gestionnaire de groupes d'activité**.
- Si vous importez des machines virtuelles qui utilisent des adresses IP statiques, préparez un pool d'adresses correctement configuré. Pour plus d'informations sur l'utilisation d'un profil réseau pour contrôler des plages d'adresses IP, reportez-vous à *Configuration de vRealize Automation*.
- Si vous utilisez l'importation en bloc pour importer une machine virtuelle avec une adresse IP statique allouée à une autre machine virtuelle, l'importation échoue.

Procédure

- 1 Désactivez temporairement tous les abonnements au service Event Broker.

Note Lors de la désactivation des abonnements, vous devez planifier une interruption de service pour votre cluster vRealize Automation. Au cours de ce processus, l'extensibilité n'est appliquée à aucune machine provisionnée normalement. L'échec de la désactivation des abonnements peut entraîner la perte de données et la suppression permanente des machines de l'infrastructure de sauvegarde.

- 2 Générez un fichier de données CSV de machine virtuelle.

- a Sélectionnez **Infrastructure > Administration > Importations en bloc**.
- b Cliquez sur **Générer le fichier CSV**.
- c Dans le menu déroulant **Machines**, sélectionnez l'option **Non géré**.
- d Dans le menu déroulant, sélectionnez la valeur par défaut **Groupe d'activité**.
- e Entrez la valeur par défaut **Propriétaire**.
- f Sélectionnez la valeur par défaut **Blueprint** dans le menu déroulant.

Le Blueprint doit être publié et ajouté à une autorisation pour que l'importation réussisse.

- g Dans le menu déroulant, sélectionnez la valeur par défaut **Machine composante**.

Si vous sélectionnez une valeur pour les options **Groupe d'activité** et **Blueprint**, les résultats suivants peuvent être visibles dans le fichier de données CSV :

- Host Reservation (Name or ID) = INVALID_RESERVATION
- Host To Storage (Name or ID) = INVALID_HOST_RESERVATION_TO_STORAGE

Ces messages s'affichent si vous ne disposez d'aucune réservation dans le groupe d'activité sélectionné pour la machine virtuelle hôte qui héberge également la machine virtuelle non gérée. Si vous avez une réservation dans ce groupe d'activité pour l'hôte de la machine virtuelle non gérée, les valeurs Réservation hôte et Hôte à stockage sont correctement renseignées.

- h Dans le menu déroulant **Ressource**, sélectionnez l'un des types de ressource disponibles.

| Option de menu | Description |
|----------------------|---|
| Point de terminaison | Informations requises pour accéder à un hôte de virtualisation. |
| Ressource de calcul | Informations requises pour accéder à un groupe de machines virtuelles remplissant une fonction similaire. |

- i Sélectionnez le nom de la ressource de machine virtuelle dans le menu déroulant **Nom**.
- j Cliquez sur **OK**.

3 Modifiez le fichier de données CSV de votre machine virtuelle.

- a Ouvrez le fichier CSV et modifiez les catégories de données pour qu'elles correspondent aux catégories existantes dans l'environnement cible de vRealize Automation.

Pour pouvoir importer les machines virtuelles contenues dans un fichier de données CSV, chaque machine virtuelle doit être associée aux éléments suivants :

- Réserveation
- Emplacement de stockage
- Blueprint
- Composant de machine virtuelle
- Propriétaire existant dans le déploiement cible

Pour que l'importation réussisse, l'ensemble des valeurs de chaque machine virtuelle doit être présent dans l'environnement vRealize Automation cible. Vous pouvez modifier les valeurs de la réserveation, l'emplacement de stockage, le Blueprint et le propriétaire ou ajouter une valeur d'adresse IP statique aux machines virtuelles en modifiant le fichier CSV.

| Titre | Commentaire |
|---------------------------------|---|
| # Import—Yes or No | Indiquez Non pour empêcher l'importation d'une machine virtuelle particulière. |
| Nom de machine virtuelle | Ne pas modifier. |
| ID de machine virtuelle | Ne pas modifier. |
| Réserveation d'hôte (Nom ou ID) | Entrez le nom ou l'ID d'une réserveation dans l'environnement vRealize Automation cible. |
| Hôte à stockage (Nom ou ID) | Entrez le nom ou l'ID d'un emplacement de stockage dans l'environnement vRealize Automation cible. |
| Nom du déploiement | Entrez un nouveau nom pour le déploiement (par exemple, nom de machine virtuelle) que vous créez dans l'environnement vRealize Automation cible. |
| | <p>Note Chaque machine virtuelle doit être importée dans son propre déploiement. Il n'est pas possible d'importer une machine virtuelle unique dans un déploiement existant. Il n'est pas possible d'importer plusieurs machines virtuelles dans un déploiement unique.</p> |
| ID du Blueprint | Entrez l'ID du Blueprint dans l'environnement vRealize Automation cible que vous utilisez pour importer la machine virtuelle. |
| | <p>Note Entrez uniquement l'ID du Blueprint, pas son nom. Vous devez sélectionner un Blueprint qui contient un seul composant de machine virtuelle. Ce Blueprint doit être publié et ajouté à un droit.</p> <p>Pour les machines virtuelles importées, n'associez pas un Blueprint qui inclut des profils de composants. Les paramètres existants des machines virtuelles importées, tels que la mémoire ou la taille de stockage, peuvent se situer en dehors des limites du profil. Dans ce cas, la validation d'une future reconfiguration basée sur le Blueprint des machines virtuelles échoue.</p> |

| Titre | Commentaire |
|--------------------------|---|
| ID de machine composante | Entrez le nom d'un composant de machine virtuelle qui est contenu dans le Blueprint que vous avez sélectionné. Il est impossible d'importer une machine virtuelle dans un Blueprint comportant plus d'un composant. |
| Nom du propriétaire | Dans l'environnement vRealize Automation cible, entrez un utilisateur disposant d'une autorisation pour le Blueprint. |

Si vous importez une machine virtuelle avec une ou plusieurs propriétés personnalisées, vous identifiez chaque propriété personnalisée à l'aide de trois valeurs séparées par des virgules ajoutées à la ligne avec les valeurs de cette machine. Utilisez ce format pour chaque propriété personnalisée.

Valeur , *Custom.Property.Name* , , *FLAGS*

FLAGS sont trois caractères qui décrivent la façon dont la propriété est traitée par vRealize Automation. Dans leur ordre d'utilisation, les indicateurs sont :

- 1 H ou N = masqué ou non masqué
- 2 E ou O = chiffré ou non chiffré
- 3 R ou P = exécution ou pas d'exécution

Par exemple, vous pouvez ajouter une propriété personnalisée pour configurer une adresse IP statique pour une machine. En utilisant le format suivant, cette propriété personnalisée attribue une adresse IP statique disponible à partir d'un profil réseau.

,VirtualMachine.Network#.Address, *w.x.y.z*, HOP

Vous modifiez les variables avec les informations correspondantes pour votre machine virtuelle.

- Remplacez le signe # par le numéro de l'interface réseau en cours de configuration avec cette adresse IP statique. Par exemple, VirtualMachine.Network0.Address.
- Remplacez *w.x.y.z* par l'adresse IP statique de la machine virtuelle. Par exemple, 11.27.42.57.

La chaîne d'indicateurs HOP (masqué, non chiffré, pas d'exécution) définit la visibilité de la propriété. Comme cette propriété particulière est utilisée uniquement par importation en bloc, elle est supprimée de la machine virtuelle après une importation réussie.

Pour que cette propriété personnalisée fonctionne, l'adresse IP doit être disponible dans un pool d'adresses correctement configuré . Si l'adresse est impossible à trouver ou est déjà utilisée, l'importation réussit sans la définition d'adresse IP statique et une erreur est journalisée.

b Enregistrez le fichier CSV.

4 Utilisez l'interface de gestion de vRealize Automation pour procéder à l'importation de votre machine virtuelle dans un environnement vRealize Automation.

- a Sélectionnez **Infrastructure > Administration > Importations en bloc**.
- b Cliquez sur **Nouveau**.

- c Entrez un nom unique pour cette tâche dans la zone de texte **Nom**, par exemple « importation non gérée 10 ».
- d Entrez le nom du fichier CSV dans la zone de texte **Fichier CSV** en accédant au nom du fichier CSV.
- e Sélectionnez des options d'importation.

| Option | Description |
|---|---|
| Heure de début | Planifiez une date de démarrage ultérieure. L'heure de début choisie est l'heure locale du serveur et non l'heure locale du poste de travail de l'utilisateur. |
| Maintenant | Le processus d'importation commence immédiatement. |
| Délai (secondes) | Si vous importez de nombreuses machines virtuelles, sélectionnez la durée en secondes séparant l'enregistrement de chaque machine virtuelle. La sélection de cette option de menu ralentit le processus d'importation. Laissez ce champ vide pour ne sélectionner aucun délai. |
| Taille du lot | Si vous importez de nombreuses machines virtuelles, sélectionnez le nombre total de machines virtuelles à enregistrer à un moment donné. La sélection de cette option de menu ralentit le processus d'importation. Laissez ce champ vide pour ne sélectionner aucune limite. |
| Ignorer les machines gérées | Ne sélectionnez pas cette option. |
| Ignorer la validation de l'utilisateur | La sélection de cette option de menu définit le propriétaire de la machine virtuelle sur la valeur répertoriée dans la colonne Propriétaire du fichier de données CSV sans vérifier si l'utilisateur existe. La sélection de cette option de menu peut réduire la durée de l'importation. |
| Tester l'importation | Testez le processus d'importation sans importer les machines virtuelles pour pouvoir vérifier que votre fichier CSV ne contient pas d'erreurs. |

- f Cliquez sur **OK**.

La progression de l'opération s'affiche sur la page Importations en bloc .

Mettre à jour une machine virtuelle dans un environnement vRealize Automation

Il est possible de modifier une propriété de machine virtuelle, comme un chemin de stockage, afin de mettre à jour une ou plusieurs machines virtuelles gérées dans un environnement vRealize Automation.

Une machine virtuelle gérée est une machine qui est gérée dans un environnement vRealize Automation et qui est visible sur la console.

Conditions préalables

- Connectez-vous à vRealize Automation en tant qu'**administrateur Fabric** et en tant que **gestionnaire de groupes d'activité**.

Procédure

- 1 Générez un fichier de données CSV de machine virtuelle.
 - a Sélectionnez **Infrastructure > Administration > Importations en bloc**.
 - b Cliquez sur **Générer le fichier CSV**.
 - c Dans le menu déroulant **Machines**, sélectionnez l'option **Géré**.
 - d Dans le menu déroulant **Ressource**, sélectionnez l'un des types de ressource disponibles.

| Option | Description |
|-----------------------------|---|
| Point de terminaison | Informations requises pour accéder à un hôte de virtualisation. |
| Ressource de calcul | Informations requises pour accéder à un groupe de machines virtuelles remplissant une fonction similaire. |

- e Sélectionnez le nom de la ressource de machine virtuelle dans le menu déroulant **Nom**.
- f (Facultatif) Sélectionnez l'option **Inclure les propriétés personnalisées** si vous voulez migrer les propriétés personnalisées de la machine virtuelle.
- g Cliquez sur **OK**.

2 Modifiez le fichier de données CSV de votre machine virtuelle.

- a Ouvrez le fichier CSV à l'aide d'un éditeur de texte et modifiez les catégories de données que vous voulez éditer de façon générale.

Pour qu'il soit possible de mettre à jour les machines virtuelles contenues dans un fichier de données CSV, chaque machine doit être associée aux éléments suivants :

- Réservation
- Emplacement de stockage
- Blueprint
- Composant de machine
- Propriétaire existant dans le déploiement cible

Pour que la mise à jour réussisse, l'ensemble des valeurs de chaque machine doit être présent dans l'environnement vRealize Automation cible. Vous pouvez modifier les valeurs de la réservation, l'emplacement de stockage, le Blueprint et le propriétaire ou ajouter une valeur d'adresse IP statique aux machines virtuelles en modifiant le fichier CSV.

- b Si vous modifiez l'adresse IP statique d'une machine virtuelle, ajoutez une commande au format suivant au fichier CSV.

```
,VirtualMachine.Network#.Address, w.x.y.z, HOP
```

Configurez la commande avec les informations correspondantes pour votre machine virtuelle.

- Remplacez le signe # par le numéro de l'interface réseau en cours de configuration avec cette adresse IP statique. Par exemple, VirtualMachineNetwork0.Address.
- Remplacez w.x.y.z par l'adresse IP statique de la machine virtuelle. Par exemple, 11.27.42.57.
- La chaîne *HOP*, Masqué, Non chiffré, Pas d'exécution, définit la visibilité de la propriété. Cette propriété par défaut est supprimée de la machine virtuelle après une importation réussie.

Pour qu'une mise à jour s'exécute avec succès, l'adresse IP doit être disponible dans un pool d'adresses configuré correctement. Si l'adresse est introuvable ou déjà utilisée, la mise à jour réussit sans la définition d'adresse IP statique et une erreur est journalisée.

- c Enregistrez le fichier CSV et fermez l'éditeur de texte.

3 Utilisez l'interface de gestion de vRealize Automation pour procéder à la mise à jour d'une ou plusieurs machines virtuelles dans un environnement vRealize Automation.

- a Sélectionnez **Infrastructure > Administration > Importations en bloc**.
- b Cliquez sur **Nouveau**.

- c Entrez un nom unique pour cette tâche dans la zone de texte **Nom**, par exemple « mise à jour globale gérée 10 ».
- d Entrez le nom du fichier CSV dans la zone de texte **Fichier CSV** en accédant au nom du fichier CSV.
- e Sélectionnez des options d'importation.

| Option | Description |
|---|---|
| Heure de début | Planifiez une date de démarrage ultérieure. L'heure de début spécifiée est l'heure locale du serveur et non l'heure locale du poste de travail de l'utilisateur. |
| Maintenant | Le processus d'importation commence immédiatement. |
| Délai (secondes) | Si vous mettez à jour un grand nombre de machines virtuelles, sélectionnez le nombre de secondes séparant la mise à jour de chaque machine virtuelle. La sélection de cette option ralentit le processus de mise à jour. Laissez ce champ vide pour ne spécifier aucun délai. |
| Taille du lot | Si vous mettez à jour un grand nombre de machines virtuelles, sélectionnez le nombre total de machines à mettre à jour à une heure donnée. La sélection de cette option ralentit le processus de mise à jour. Laissez ce champ vide pour ne spécifier aucune limite. |
| Ignorer les machines gérées | Ne sélectionnez pas cette option. |
| Ignorer la validation de l'utilisateur | La sélection de cette option définit le propriétaire de la machine sur la valeur répertoriée dans la colonne Propriétaire du fichier de données CSV sans vérifier si l'utilisateur existe. La sélection de cette option peut réduire la durée de la mise à jour. |
| Tester l'importation | Ne sélectionnez pas cette option. |

- f Cliquez sur **OK**.

La progression de l'opération s'affiche sur la page Importations en bloc.

Migrer une machine virtuelle vers un autre environnement vRealize Automation

Il est possible de migrer une ou plusieurs machines virtuelles gérées d'un environnement VMware vRealize™ Automation vers un autre environnement vRealize Automation.

Une machine virtuelle gérée est une machine virtuelle qui est gérée dans un environnement vRealize Automation et qui est visible sur la console.

Conditions préalables

- Connectez-vous à vRealize Automation en tant qu'**administrateur Fabric** et en tant que **gestionnaire de groupes d'activité**.

- Si vous importez des machines virtuelles qui utilisent des adresses IP statiques, préparez un pool d'adresses correctement configuré. Pour plus d'informations sur l'utilisation d'un profil réseau pour contrôler des plages d'adresses IP, reportez-vous à *Configuration de vRealize Automation*.

Procédure

- 1 Générez un fichier de données CSV de machine virtuelle.
 - a Sélectionnez **Infrastructure > Administration > Importations en bloc**.
 - b Cliquez sur **Générer le fichier CSV**.
 - c Dans le menu déroulant **Machines**, sélectionnez l'option **Géré**.
 - d Dans le menu déroulant **Ressource**, sélectionnez l'un des types de ressource disponibles.

| Option | Description |
|-----------------------------|---|
| Point de terminaison | Informations requises pour accéder à un hôte de virtualisation. |
| Ressource de calcul | Informations requises pour accéder à un groupe de machines virtuelles remplissant une fonction similaire. |

- e Sélectionnez le nom de la ressource de machine virtuelle dans le menu déroulant **Nom**.
- f (Facultatif) Sélectionnez l'option **Inclure les propriétés personnalisées**.
 Vous incluez des propriétés personnalisées lorsque vous importez une machine virtuelle dans un nouveau déploiement avec les mêmes propriétés.
- g Cliquez sur **OK**.

2 Modifiez le fichier de données CSV de votre machine virtuelle.

La nécessité de modifier le fichier de données CSV dépend de la similitude des environnements source et cible. Si les valeurs de configuration de l'environnement source ne correspondent pas aux valeurs de l'environnement cible, vous devez modifier le fichier de données CSV afin que les valeurs concordent avant de commencer la migration.

- a Ouvrez le fichier CSV et modifiez les catégories de données pour qu'elles correspondent aux catégories existantes dans l'environnement cible de vRealize Automation.

Pour effectuer la migration de machines virtuelles contenues dans un fichier de données CSV, chaque machine virtuelle doit être associée à une réservation, un emplacement de stockage, un Blueprint, un composant de machine et un propriétaire existant dans l'environnement vRealize Automation cible. Pour que la migration réussisse, l'ensemble des valeurs de chaque machine virtuelle doit être présent dans l'environnement vRealize Automation cible. Vous pouvez modifier les valeurs de la réservation, l'emplacement de stockage, le Blueprint et le propriétaire ou ajouter une valeur d'adresse IP statique aux machines virtuelles en modifiant le fichier CSV.

| Titre | Commentaire | Exemple |
|--------------------------------|--|---------------------------------------|
| N° d'importation -Oui ou Non | Indiquez Non pour empêcher l'importation d'une machine virtuelle particulière. | Oui |
| Nom de machine virtuelle | Ne pas modifier. | MyMachine |
| ID de machine virtuelle | Ne pas modifier. | a6e05812-0b06-4d4e-a84a-fed242340426a |
| Réservation d'hôte (Nom ou ID) | Entrez le nom ou l'ID d'une réservation dans l'environnement vRealize Automation cible. | DevReservation |
| Hôte à stockage (Nom ou ID) | Entrez le nom ou l'ID d'un emplacement de stockage dans l'environnement vRealize Automation cible. | ce-san-1:custom-nfs-2 |
| Nom du déploiement | Entrez un nouveau nom pour le déploiement que vous créez dans l'environnement vRealize Automation cible. Chaque machine virtuelle doit migrer vers son propre déploiement. Il n'est pas possible d'importer une machine virtuelle unique dans un déploiement existant. Il n'est pas possible d'importer plusieurs machines virtuelles dans un environnement unique. | ImportedDeployment0001 |
| ID de Blueprint convergé | Entrez l'ID du Blueprint dans l'environnement vRealize Automation cible que vous utilisez pour importer la machine virtuelle. Assurez-vous d'entrer uniquement l'ID du Blueprint. N'entrez pas le nom du Blueprint. Vous devez sélectionner un Blueprint qui contient un seul composant de machine virtuelle. Ce Blueprint doit être publié et ajouté à un droit. | ImportBlueprint |

| Titre | Commentaire | Exemple |
|------------------------------|---|-----------------|
| ID de Blueprint de composant | Entrez le nom d'un composant de machine virtuelle qui est contenu dans le Blueprint que vous avez sélectionné. Il est impossible d'importer une machine virtuelle dans un Blueprint comportant plus d'un composant. | ImportedMachine |
| Nom du propriétaire | Entrez un utilisateur dans l'environnement vRealize Automation cible. | user@tenant |

Exemple d'une ligne CSV complète, correctement formatée : Yes, MyMachine, a6e05812-0b06-4d4e-a84a-fed242340426, DevReservation, ce-san-1:custom-nfs-2, Imported Deployment 0001, ImportBlueprint, ImportedMachine, user@tenant

- b Si vous migrez une machine virtuelle avec une adresse IP statique, ajoutez une commande au format suivant au fichier CSV.

```
,VirtualMachine.Network#.Address, w.x.y.z, HOP
```

Configurez la commande avec les informations correspondantes pour votre machine virtuelle.

- Remplacez le signe # par le numéro de l'interface réseau en cours de configuration avec cette adresse IP statique. Par exemple, VirtualMachineNetwork0.Address.
- Remplacez w.x.y.z par l'adresse IP statique de la machine virtuelle. Par exemple, 11.27.42.57.
- La chaîne *HOP*, Masqué, Non chiffré, Pas d'exécution, définit la visibilité de la propriété. Cette propriété par défaut est supprimée de la machine virtuelle après une importation réussie.

Pour qu'une migration s'exécute avec succès, l'adresse IP doit être disponible dans un pool d'adresses configuré correctement. Si l'adresse est introuvable ou déjà utilisée, la migration réussit sans la définition d'adresse IP statique et une erreur est journalisée.

- c Enregistrez le fichier CSV.

- 3 Utilisez l'interface de gestion de vRealize Automation pour procéder à la migration de votre machine virtuelle vers un environnement vRealize Automation.

- a Sélectionnez **Infrastructure > Administration > Importations en bloc**.
- b Cliquez sur **Nouveau**.
- c Entrez un nom unique pour cette tâche dans la zone de texte **Nom**, par exemple « migration gérée 10 ».
- d Entrez le nom du fichier CSV dans la zone de texte **Fichier CSV** en accédant au nom du fichier CSV.

- e Sélectionnez des options d'importation.

| Option | Description |
|---|---|
| Heure de début | Planifiez une date de démarrage ultérieure. L'heure de début choisie est l'heure locale du serveur et non l'heure locale du poste de travail de l'utilisateur. |
| Maintenant | Le processus de migration commence immédiatement. |
| Délai (secondes) | Si vous effectuez la migration de nombreuses machines virtuelles, sélectionnez la durée en secondes séparant l'enregistrement de chaque machine virtuelle. La sélection de cette option ralentit le processus de migration. Laissez ce champ vide pour ne sélectionner aucun délai. |
| Taille du lot | Si vous effectuez la migration de nombreuses machines virtuelles, sélectionnez le nombre total de machines virtuelles à enregistrer à un moment donné. La sélection de cette option ralentit le processus de migration. Laissez ce champ vide pour ne sélectionner aucune limite. |
| Ignorer les machines gérées | Ne sélectionnez pas cette option. |
| Ignorer la validation de l'utilisateur | La sélection de cette option définit le propriétaire de la machine virtuelle sur la valeur répertoriée dans la colonne Propriétaire du fichier de données CSV sans vérifier si l'utilisateur existe. La sélection de cette option peut réduire la durée de la migration. |
| Tester l'importation | Testez le processus de migration sans migrer les machines virtuelles pour pouvoir vérifier que votre fichier CSV ne contient pas d'erreurs. |

- f Cliquez sur **OK**.

La progression de l'opération s'affiche sur la page Importations en bloc.