Installation et configuration de VMware vRealize Orchestrator

Février 2022

vRealize Orchestrator 8.7

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

Table des matières

Installation et configuration de VMware vRealize Orchestrator

La section *Installation et configuration de VMware vRealize Orchestrator* fournit des informations et des instructions sur l'installation et la configuration de VMware® vRealize Orchestrator.

Public visé

Ces informations s'adressent à des administrateurs vSphere avancés et à des administrateurs système qui connaissent la technologie des machines virtuelles et le fonctionnement des centres de données.

Introduction à VMware vRealize Orchestrator

1

VMware vRealize Orchestrator est une plate-forme d'automatisation des processus et du développement qui fournit une bibliothèque de workflows extensibles vous permettant de créer et d'exécuter des processus configurables automatisés pour gérer les produits VMware, ainsi que d'autres technologies tierces.

vRealize Orchestrator automatise la gestion et les tâches opérationnelles pour VMware comme pour les applications tierces, comme les centres d'assistance, les systèmes de gestion des modifications et les systèmes de gestion des ressources informatiques.

Ce chapitre contient les rubriques suivantes :

Fonctionnalités clés de la plate-forme Orchestrator

vRealize Orchestrator est constitué de trois couches distinctes : une plate-forme d'orchestration qui offre les fonctionnalités courantes requises dans un outil d'orchestration, une architecture de plug-in pour intégrer le contrôle des sous-systèmes et une bibliothèque de workflows. vRealize Orchestrator est une plate-forme ouverte offrant des capacités d'extension aux nouveaux plug-ins et contenus, et peut être intégré à des architectures plus vastes via une API REST.

vRealize Orchestrator inclut plusieurs fonctionnalités clés qui facilitent l'exécution et la gestion des workflows.

Persistance

Une base de données PostgreSQL de niveau production est utilisée pour stocker des informations pertinentes (comme des processus, des états des workflows et la configuration de vRealize Orchestrator).

Gestion centralisée

Avec vRealize Orchestrator, la gestion des processus est centralisée. La plate-forme basée sur serveur d'applications et pourvue d'un historique complet des versions peut stocker les scripts

et les primitives relatives aux processus dans un même emplacement de stockage. De cette façon, vous pouvez éviter les scripts sans contrôle de version, ni historique des modifications en bonne et due forme sur vos serveurs.

Réalisation de points de contrôle

Chaque étape d'un workflow est enregistrée dans la base de données, ce qui empêche toute perte de données si vous devez redémarrer le serveur. Cette fonctionnalité est particulièrement utile pour les processus au long cours.

Centre de contrôle

Le centre de contrôle est un portail Web qui accroît l'efficacité de l'administration des instances de vRealize Orchestrator en proposant une interface d'administration centralisée pour les opérations en cours d'exécution, la surveillance des workflows, ainsi que la corrélation entre les workflows qui s'exécutent et les ressources du système.

Contrôle de version

Tous les objets de la plate-forme vRealize Orchestrator se voient associer un historique des versions. L'historique des versions s'avère utile pour la gestion basique des modifications lorsqu'il s'agit de distribuer des processus à des étapes ou des emplacements du projet.

Intégration Git

Avec vRealize Orchestrator Client, vous pouvez intégrer un référentiel Git pour améliorer le contrôle de version et de source de votre contenu vRealize Orchestrator. Avec Git, vous pouvez gérer le développement de workflows sur plusieurs instances de vRealize Orchestrator. Reportez-vous à *Utilisation de Git avec vRealize Orchestrator Client* dans le guide *Utilisation de VMware vRealize Orchestrator Client*.

Moteur de scripts

Le moteur JavaScript Mozilla Rhino procure un moyen de créer des blocs constitutifs pour la plate-forme vRealize Orchestrator Client. Le moteur de scripts est enrichi par un contrôle basique des versions, la vérification des types de variable, la gestion des espaces de nom et le traitement des exceptions. Le moteur peut être utilisé dans les blocs constitutifs suivants :

- Actions
- Workflows
- Stratégies

Moteur de workflow

Le moteur de workflow vous permet d'automatiser les processus d'activité. Il se sert des objets suivants pour créer une automatisation des processus étape par étape dans les workflows :

- Les workflows et les actions que vRealize Orchestrator Client propose.
- Les blocs constitutifs personnalisés créés par le client.
- Les objets que les plug-ins ajoutent à vRealize Orchestrator Client.

Les utilisateurs, d'autres workflows, des planifications ou des stratégies peuvent démarrer les workflows.

Moteur de stratégies

Vous pouvez utiliser le moteur de stratégies pour surveiller et générer des événements afin de réagir à des changements de conditions dans le serveur vRealize Orchestrator Client ou la technologie en plug-in. Les stratégies peuvent regrouper les événements issus de la plate-forme ou des plug-ins, ce qui vous permet de traiter les changements de conditions dans l'une quelconque des technologies intégrées.

vRealize Orchestrator Client

Créez, exécutez, modifiez et surveillez les workflows avec vRealize Orchestrator Client. Vous pouvez également utiliser vRealize Orchestrator Client pour gérer des éléments d'action, de configuration, de stratégie et de ressource. Reportez-vous à *Utilisation de vRealize Orchestrator Client*.

Développement et ressources

La page de lancement de vRealize Orchestrator fournit un accès rapide aux ressources pour vous aider à développer vos propres plug-ins, afin de les utiliser dans vRealize Orchestrator. Vous trouverez également des informations sur l'utilisation de l'API REST de vRealize Orchestrator pour envoyer des demandes au serveur vRealize Orchestrator.

Sécurité

vRealize Orchestrator offre les fonctions de sécurité avancées ci-dessous :

- Un mécanisme PKI (infrastructure de clé publique) pour signer et chiffrer le contenu importé et exporté d'un serveur à l'autre.
- Un mécanisme DRM (gestion des droits numériques) pour contrôler de quelle façon le contenu exporté peut être visualisé, modifié ou redistribué.
- TLS (Transport Layer Security) pour fournir des communications chiffrées entre vRealize Orchestrator Client, le serveur vRealize Orchestrator et l'accès HTTPS au frontal Web.
- Une gestion avancée des droits d'accès pour assurer un contrôle sur l'accès aux processus et sur les objets manipulés par ces processus.

Chiffrement

vRealize Orchestrator utilise la technologie de chiffrement conforme aux FIPS AES (Advanced Encryption Standard) avec une clé 256 bits pour le chiffrement des chaînes. La clé de chiffrement est générée de façon aléatoire et unique sur l'ensemble des appliances n'appartenant pas à un cluster. Tous les nœuds d'un cluster partagent la même clé de chiffrement.

Rôles d'utilisateur de vRealize Orchestrator

vRealize Orchestrator propose différents outils et interfaces en fonction des responsabilités spécifiques des rôles d'utilisateurs globaux. Dans vRealize Orchestrator, vous pouvez avoir des utilisateurs disposant de droits complets, qui font partie du groupe d'administrateurs (**administrators**), de développeurs (**workflow designers**), d'utilisateurs pour le dépannage (**viewers**) et des utilisateurs disposant de droits limités.

Les rôles d'utilisateur de vRealize Orchestrator sont gérés dans le menu **Gestion des rôles** de vRealize Orchestrator Client. Pour plus d'informations sur la configuration des rôles d'utilisateur dans le vRealize Orchestrator Client, reportez-vous à la section *Attribuer des rôles dans le client vRealize Orchestrator* du guide *Utilisation du client VMware vRealize Orchestrator*.

Note Pour les déploiements vRealize Orchestrator authentifiés avec vRealize Automation ou à l'aide d'une licence vRealize Automation, les rôles d'utilisateur sont attribués avec le service de gestion des identités et des accès de la plate-forme vRealize Automation. Reportez-vous à *Configurer des rôles de vRealize Orchestrator Client dans vRealize Automation* dans *Utilisation de VMware vRealize Orchestrator Client*.

Rôle d'utilisateur	Description
Administrateur	Cet utilisateur dispose d'un accès complet à l'ensemble des fonctionnalités et du contenu de la plate-forme vRealize Orchestrator, y compris le contenu créé par des groupes spécifiques. Les principales responsabilités de l'administrateur sont les suivantes : ■ Installation et configuration de vRealize Orchestrator. ■ Ajout d'utilisateurs au vRealize Orchestrator Client, attribution de rôles, création et suppression de groupes. Reportez-vous à la section *Créer des groupes dans vRealize Orchestrator Client* dans *Utilisation de VMware vRealize Orchestrator Client*. ■ Création d'une intégration avec un référentiel Git pour les développeurs dans leur environnement vRealize Orchestrator. Reportez-vous à la section *Configurer une connexion à un référentiel Git* dans *Utilisation de VMware vRealize Orchestrator Client*. ■ Dépannage de leur environnement vRealize Orchestrator via des fonctionnalités telles que la validation des workflows et le débogage des scripts de workflow.
Observateur	Cet utilisateur dispose d'un accès en lecture seule à toutes les instances de vRealize Orchestrator Client, y compris tous les groupes et le contenu des groupes. Il peut afficher, mais ne peut pas créer, modifier, ni exécuter du contenu, ou exporter des exécutions de workflow, des journaux d'exécution de workflow ou des modules. Les utilisateurs ne sont pas limités par les autorisations de groupe. **Note** Le rôle d'observateur est pris en charge uniquement pour les instances de vRealize Orchestrator authentifiées dans vRealize Automation. Ce rôle n'est pas mappé à un rôle vRealize Automation par défaut. Vous devez donc l'attribuer aux utilisateurs de manière explicite.

Rôle d'utilisateur	Description
Concepteur de workflow	Cet utilisateur peut étendre la fonctionnalité de la plate-forme vRealize Orchestrator en créant et en modifiant des objets. Les concepteurs de workflow n'ont pas accès aux fonctionnalités d'administration et de dépannage de vRealize Orchestrator Client. Les principales responsabilités du concepteur de workflow sont les suivantes : ■ Création, modification, exécution et suppression d'objets vRealize Orchestrator, tels que les workflows, les actions, les stratégies et les éléments de configuration. ■ Planification des exécutions de workflow. Consultez *Planifier des workflows dans vRealize Orchestrator Client* dans *Utilisation de VMware vRealize Orchestrator Client*. ■ Ajout de contenu créé par le développeur de workflow aux groupes auxquels ils sont attribués. ■ Transfert des modifications locales apportées à l'inventaire de contenu vRealize Orchestrator vers le référentiel Git connecté. Voir *Transférer les modifications vers un référentiel* dans *Utilisation de VMware vRealize Orchestrator Client*.
Utilisateurs aux droits limités	Les utilisateurs sans rôle attribué peuvent toujours se connecter à vRealize Orchestrator Client, mais ils ont un accès limité aux fonctionnalités et au contenu du client. S'ils sont associés à un groupe, ils peuvent afficher et exécuter le contenu inclus dans ce groupe.

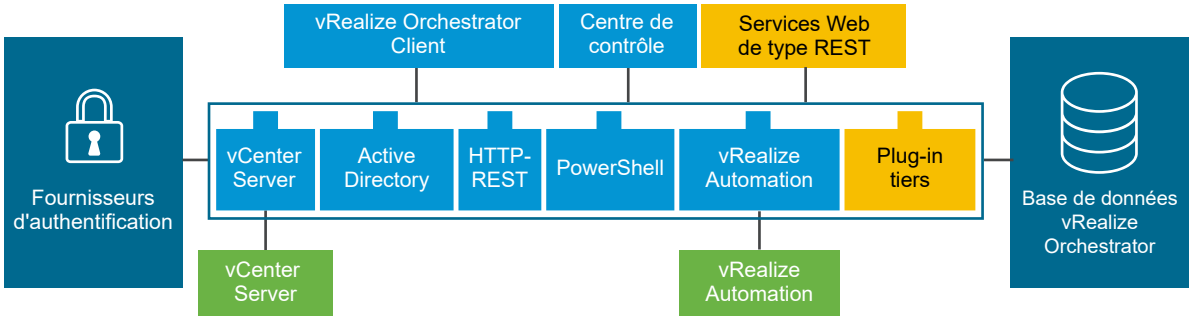
Architecture de vRealize Orchestrator

vRealize Orchestrator contient une bibliothèque de workflows et un moteur de workflow qui vous permettent de créer et d'exécuter des workflows afin d'automatiser les processus d'orchestration. Vous exécutez les workflows sur les objets des différentes technologies auxquelles vRealize Orchestrator accède via une série de plug-ins.

vRealize Orchestrator fournit un jeu standard de plug-ins, dont ceux concernant vCenter Server et vRealize Automation, pour vous permettre d'orchestrer les tâches dans les différents environnements que le plug-in expose.

vRealize Orchestrator présente aussi une architecture ouverte permettant de brancher des applications tierces à la plate-forme d'orchestration. Vous avez la possibilité d'exécuter des workflows sur les objets des technologies en plug-in que vous définissez vous-même. vRealize Orchestrator est relié à un fournisseur d'authentification pour la gestion des comptes utilisateurs et à une base de données PostgreSQL préconfigurée pour le stockage des informations issues des workflows qu'il exécute. Vous pouvez accéder à vRealize Orchestrator, aux objets qu'il expose et aux workflows de vRealize Orchestrator via l'interface du vRealize Orchestrator Client ou via les services Web. La surveillance et la configuration des services et des workflows de vRealize Orchestrator s'effectuent via le vRealize Orchestrator Client et le centre de contrôle.

Figure 1-1. Architecture de VMware vRealize Orchestrator



vRealize Orchestrator Plug-ins

Les plug-ins vous permettent d'utiliser vRealize Orchestrator pour accéder à des technologies et à des applications externes, et pour les contrôler. En exposant une technologie externe dans un plug-in vRealize Orchestrator, vous pouvez incorporer des objets et des fonctions aux workflows qui accèdent aux objets et aux fonctions de cette technologie externe.

Les technologies externes auxquelles vous pouvez accéder en utilisant des plug-ins incluent des outils de gestion de virtualisation, des systèmes de messagerie, des bases de données, des services d'annuaire et des interfaces de contrôle à distance.

vRealize Orchestrator fournit un ensemble de plug-ins standard que vous pouvez utiliser pour intégrer des technologies telles que les API VMware vCenter Server et des fonctionnalités de messagerie à des workflows. Avec les plug-ins, vous pouvez automatiser la livraison de nouveaux services informatiques ou adapter les fonctionnalités de l'infrastructure et des services applicatifs existants. Vous pouvez également utiliser l'architecture modulaire ouverte de vRealize Orchestrator pour développer des plug-ins afin d'accéder à d'autres applications.

Les plug-ins vRealize Orchestrator développés par VMware sont distribués sous forme de fichiers `.vmoapp`.

Pour en savoir plus sur les plug-ins vRealize Orchestrator, reportez-vous à la section Utilisation des plug-ins VMware vRealize Orchestrator.

Pour en savoir plus sur les plug-ins vRealize Orchestrator tiers, reportez-vous à VMware Marketplace.

Configuration requise du système pour vRealize Orchestrator 2

Votre système doit satisfaire aux conditions requises techniques nécessaires au fonctionnement correct de vRealize Orchestrator.

Pour connaître la liste des versions prises en charge de vCenter Server, vSphere Web Client, vRealize Automation et des autres solutions VMware, consultez la Matrice d'interopérabilité des produits VMware.

Ce chapitre contient les rubriques suivantes :

- Composants du dispositif vRealize Orchestrator Appliance
- Configuration matérielle requise pour le dispositif vRealize Orchestrator Appliance
- Valeurs maximales d'évolutivité de vRealize Orchestrator
- Configuration réseau requise pour vRealize Orchestrator
- Ports et points de terminaison vRealize Orchestrator
- Navigateurs pris en charge par vRealize Orchestrator
- Niveau de prise en charge de l'internationalisation et de la localisation

Composants du dispositif vRealize Orchestrator Appliance

vRealize Orchestrator Appliance est un dispositif virtuel basé sur Photon exécuté dans des conteneurs.

Le dispositif vRealize Orchestrator Appliance inclut les composants suivants :

- Une couche Kubernetes de niveau infrastructure.
- Une base de données PostgreSQL préconfigurée.
- Les services de base vRealize Orchestrator : le service du serveur, le service du centre de contrôle et le service de l'interface utilisateur d'orchestration.

La configuration de base de données par défaut d'vRealize Orchestrator Appliance est compatible avec les environnements de production.

Note Pour utiliser le dispositif vRealize Orchestrator Appliance dans un environnement de production, vous devez configurer le serveur vRealize Orchestrator pour qu'il s'authentifie via vRealize Automation ou vSphere. Voir Configuration d'un serveur vRealize Orchestrator autonome.

Configuration matérielle requise pour le dispositif vRealize Orchestrator Appliance

Le dispositif vRealize Orchestrator Appliance est une machine virtuelle basée sur Photon préconfigurée qui s'exécute dans des conteneurs. Avant de déployer le dispositif, vérifiez que votre système dispose de la configuration matérielle minimale requise.

Le dispositif vRealize Orchestrator Appliance nécessite la configuration matérielle suivante :

- 4 CPU
- 12 Go de mémoire
- 200 Go de disque dur

Ne réduisez pas la taille de la mémoire par défaut, car le serveur vRealize Orchestrator nécessite au moins 8 Go de mémoire libre.

Valeurs maximales d'évolutivité de vRealize Orchestrator

Le tableau des limites d'évolutivité décrit les valeurs maximales recommandées pour les déploiements de vRealize Orchestrator 8.x.

Composant	Cibles d'échelle	Plus d'informations
Machines virtuelles	35 000	
Connexions à l'instance de vCenter Server	10	Voir Configuration de vCenter Server
Les nodes actifs dans un cluster	3	Voir Configurer un cluster vRealize Orchestrator
Workflows exécutés simultanément	300 par nœud	Voir Configuration des propriétés d'exécution de workflow
Workflows en cours d'exécution mis en file d'attente	10 000 par nœud	
Exécutions de workflow conservées	100 par nœud	
Jours d'expiration des événements du journal	15	

Configuration réseau requise pour vRealize Orchestrator

Chaque nœud vRealize Orchestrator nécessite une configuration réseau.

La configuration réseau requise pour vRealize Orchestrator est la suivante :

- Adresse réseau et IPv4 statique unique
- Serveur DNS accessible défini manuellement
- Nom de domaine complet (FQDN) valide défini manuellement dont la résolution peut être directe et inversée via le serveur DNS

Note La modification de l'adresse IP ou du nom d'hôte après l'installation n'est pas prise en charge et entraîne une interruption de la configuration irrécupérable.

Ports et points de terminaison vRealize Orchestrator

Le service vRealize Orchestrator Kubernetes comporte deux points de terminaison et plusieurs ports réseau principaux.

Ports réseau de vRealize Orchestrator

Vous pouvez accéder à vRealize Orchestrator sur le port 443. Le port 443 est sécurisé avec un certificat auto-signé généré lors de l'installation. Lors de l'utilisation d'un équilibrage de charge externe, il doit être configuré pour équilibrer le port 443.

Pour afficher tous les ports vRealize Orchestrator, reportez-vous à l'outil Ports and Protocols.

Points de terminaison vRealize Orchestrator

Vous pouvez accéder au client vRealize Orchestrator et aux services du centre de contrôle sur les points de terminaison suivants.

Service	Point de terminaison
Client vRealize Orchestrator	`https://your_orchestrator_FQDN/orchestration-ui`
Centre de contrôle	`https://your_orchestrator_FQDN/vco-controlcenter`

Navigateurs pris en charge par vRealize Orchestrator

Vérifiez que vos navigateurs prennent en charge vRealize Orchestrator.

Pour accéder à vRealize Orchestrator Client et au centre de contrôle, vous devez utiliser l'un des navigateurs suivants :

- Microsoft Edge
- Mozilla Firefox

- Google Chrome

Niveau de prise en charge de l'internationalisation et de la localisation

Le centre de contrôle vRealize Orchestrator et vRealize Orchestrator Client prennent en charge les systèmes d'exploitation et la mise en forme des données pour des langues autres que l'anglais, ainsi que la prise en charge multilingue pour le centre de contrôle et l'interface utilisateur du client.

Le centre de contrôle vRealize Orchestrator et vRealize Orchestrator Client prennent en charge l'utilisation de systèmes d'exploitation, l'entrée et la sortie, ainsi que la prise en charge de données pour des langues autres que l'anglais, telles que les dates, l'heure et les chiffres.

Les interfaces utilisateur de vRealize Orchestrator et du vRealize Orchestrator Client sont localisées dans les langues suivantes :

- Espagnol
- Français
- Allemand
- Chinois traditionnel
- Chinois simplifié
- Coréen
- Japonais
- Italian
- Néerlandais
- Portugais (Brésil)
- Russian

Installation des composants vRealize Orchestrator 3

Lorsque vous téléchargez et déployez le dispositif vRealize Orchestrator Appliance, le serveur vRealize Orchestrator est préconfiguré. Après le déploiement, le service démarre automatiquement.

Pour améliorer la disponibilité et l'évolutivité de votre configuration de vRealize Orchestrator, suivez les instructions suivantes :

- Installez et configurez un fournisseur d'authentification et configurez vRealize Orchestrator pour qu'il fonctionne avec ce fournisseur. Reportez-vous à Configuration d'un serveur vRealize Orchestrator autonome.
- Pour les environnements vRealize Orchestrator en cluster, installez et un serveur d'équilibrage de charge et configurez-le afin de distribuer la charge de travail entre les serveurs vRealize Orchestrator.

Ce chapitre contient les rubriques suivantes :

Configuration de vCenter Server

L'augmentation du nombre d'instances de vCenter Server dans votre configuration vRealize Orchestrator pousse vRealize Orchestrator à gérer des sessions supplémentaires. Trop de sessions actives peuvent entraîner des délais d'expiration de vRealize Orchestrator si plus de 10 connexions vCenter Server se produisent.

Pour connaître la liste des versions de vCenter Server prises en charge, consultez la page Matrice d'interopérabilité des produits VMware.

Note Si votre réseau dispose d'une bande passante et d'une latence suffisantes, vous pouvez exécuter plusieurs instances de vCenter Server sur différentes machines virtuelles dans votre configuration vRealize Orchestrator. Si vous utilisez le LAN pour améliorer la communication entre vRealize Orchestrator et vCenter Server, une ligne de 100 Mo est obligatoire.

Méthodes d'authentification

Pour authentifier et gérer les autorisations d'utilisateur, vRealize Orchestrator nécessite une connexion à vRealize Automation ou à une instance de serveur vSphere.

Lorsque vous téléchargez et déployez le dispositif vRealize Orchestrator Appliance, vous devez configurer le serveur avec une authentification vRealize Automation ou vSphere. Reportez-vous à Configuration d'un serveur vRealize Orchestrator autonome.

Note L'authentification vRealize Orchestrator 8.x avec vRealize Automation est uniquement prise en charge avec vRealize Automation 8.x.

Installation de vRealize Orchestrator

4

vRealize Orchestrator est constitué d'un composant serveur et d'un composant client.

Pour utiliser vRealize Orchestrator, vous devez déployer le dispositif vRealize Orchestrator Appliance et configurer le serveur vRealize Orchestrator.

Vous pouvez modifier les paramètres de configuration de vRealize Orchestrator par défaut via le centre de contrôle vRealize Orchestrator.

Ce chapitre contient les rubriques suivantes :

Télécharger et déployer le dispositif vRealize Orchestrator Appliance

Avant de pouvoir accéder au contenu et aux services vRealize Orchestrator, vous devez télécharger et déployer le dispositif vRealize Orchestrator Appliance.

Conditions préalables

- Vérifiez que vous disposez d'une instance valide de vCenter Server. La version de vCenter Server doit être 6.0 ou une version ultérieure.
- Vérifiez que l'hôte sur lequel vous déployez le dispositif vRealize Orchestrator Appliance répond à la configuration matérielle minimale. Reportez-vous à Configuration matérielle requise pour le dispositif vRealize Orchestrator Appliance.
- Si votre système est isolé et n'est pas connecté à Internet, vous devez télécharger le fichier `.ova` du dispositif à partir du site Web de VMware.

Procédure

1. Connectez-vous à vSphere Web Client en tant qu'**administrateur**.
2. Sélectionnez un objet d'inventaire correspondant à un objet parent valide d'une machine virtuelle, tel qu'un centre de données, un dossier, un cluster, un pool de ressources ou un hôte.
3. Sélectionnez **Actions > Déployer le modèle OVF**.
4. Entrez le chemin ou l'URL vers le fichier `.ova` et cliquez sur **Suivant**.

5 Entrez un nom et un emplacement pour le dispositif vRealize Orchestrator Appliance déployé, puis cliquez sur **Suivant**.

6 Sélectionnez un hôte, un cluster, un pool de ressources ou vApp comme destination sur laquelle vous souhaitez que le dispositif s'exécute, puis cliquez sur **Suivant**.

7 Vérifiez les détails du déploiement et cliquez sur **Suivant**.

8 Acceptez les termes du contrat de licence et cliquez sur **Suivant**.

9 Sélectionnez le format de stockage à utiliser pour le dispositif vRealize Orchestrator Appliance.

Format	Description
Provisionnement statique mis à zéro en différé	Crée un disque virtuel au format statique par défaut. L'espace nécessaire pour le disque virtuel est alloué lorsque le disque virtuel est créé. Toutes les données qui demeurent sur le périphérique physique ne sont pas effacées pendant la création, mais sont mises à zéro sur demande à la première écriture sur la machine virtuelle.
Provisionnement statique mis à zéro immédiatement	Prend en charge les fonctionnalités de clustering telles que la tolérance de panne. L'espace nécessaire pour le disque virtuel est alloué lorsque le disque virtuel est créé. Les données qui restent sur le périphérique physique sont mises à zéro lors de la création du disque virtuel. La création de disques à ce format peut être beaucoup plus longue que pour d'autres formats.
Format de provisionnement dynamique	Économise de l'espace disque. Pour le disque dynamique, vous fournissez autant d'espace de banque de données que le disque en exigerait d'après la valeur que vous sélectionnez comme taille de disque. Le disque dynamique démarre avec un petit espace et il utilise au début uniquement l'espace de banque de données dont il a besoin pour ses opérations initiales.

10 Cliquez sur **Suivant**.

11 Configurez les paramètres réseau et entrez le mot de passe **root**.

Lorsque vous configurez les paramètres réseau du dispositif vRealize Orchestrator Appliance, vous devez utiliser le protocole IPv4. Pour les configurations de réseau DHCP et statique, vous devez ajouter un nom de domaine complet (FQDN) pour votre dispositif vRealize Orchestrator Appliance.

Si le nom d'hôte affiché dans le shell du dispositif vRealize Orchestrator Appliance déployé est *photon-machine*, la configuration réseau requise précédente n'est pas respectée.

12 (Facultatif) Configurez des paramètres réseau supplémentaires pour vRealize Orchestrator Appliance, tels que l'activation de l'accès SSH.

Note Lors de la configuration d'un réseau Kubernetes, les valeurs du CIDR de cluster interne et du CIDR de service interne doivent autoriser au moins 1 024 hôtes. En raison de cette condition requise, la valeur de masque de réseau doit être de 22 au maximum. Les valeurs de masque de réseau supérieures à 22 ne sont pas valides. Les propriétés du réseau Kubernetes doivent comporter les valeurs par défaut suivantes :

Kubernetes network property	Default value	Property description
CIDR de cluster interne Kubernetes	10.244.0.0/22	CIDR utilisé pour les espaces s'exécutant dans le cluster Kubernetes.
CIDR de service interne Kubernetes	10.244.4.0/22	CIDR utilisé pour les services Kubernetes dans le cluster Kubernetes.

Note Vous pouvez également modifier les propriétés réseau du CIDR Kubernetes après le déploiement. Reportez-vous à Configurer le CIDR Kubernetes de vRealize Orchestrator.

13 (Facultatif) Pour activer le mode FIPS pour vRealize Orchestrator Appliance, définissez **Mode FIPS** sur **`strict`**.

Note L'activation de FIPS 140-2 est uniquement prise en charge pour les environnements vRealize Orchestrator. Si vous souhaitez activer le mode FIPS sur votre environnement, vous devez le faire pendant l'installation.

14 Cliquez sur **Suivant**.

15 Vérifiez la page **Prêt à terminer** et cliquez sur **Terminer**.

Résultats

Le vRealize Orchestrator Appliance est correctement déployé.

Étape suivante

Connectez-vous à la ligne de commande du dispositif vRealize Orchestrator Appliance en tant que **root** et confirmez que vous pouvez effectuer une recherche DNS directe ou inversée.

- Pour effectuer une recherche DNS directe, exécutez la commande `nslookup` *your_orchestrator_FQDN*. La commande doit renvoyer l'adresse IP du dispositif vRealize Orchestrator Appliance.
- Pour effectuer une recherche DNS inversée, exécutez la commande `nslookup` *your_orchestrator_IP*. La commande doit renvoyer le nom de domaine complet du dispositif vRealize Orchestrator Appliance.

Note Si vous n'avez pas activé SSH pendant le déploiement, vous pouvez également effectuer des recherches DNS à partir de la console de machine virtuelle dans vSphere Web Client.

Mettre sous tension le dispositif vRealize Orchestrator et ouvrir la page d'accueil

Pour utiliser l'instance autonome de vRealize Orchestrator Appliance, vous devez d'abord le mettre sous tension.

Procédure

1. Connectez-vous à vSphere Web Client en tant qu'**administrateur**.
2. Cliquez avec le bouton droit sur le dispositif vRealize Orchestrator Appliance et sélectionnez **Alimentation > Mettre sous tension**.
3. Dans un navigateur Web, accédez à l'adresse d'hôte de votre machine virtuelle vRealize Orchestrator Appliance que vous avez configurée pendant le déploiement OVA.

   https://*your_orchestrator_FQDN*/vco.

Activer ou désactiver l'accès SSH au dispositif vRealize Orchestrator Appliance

Vous pouvez activer ou désactiver l'accès SSH au dispositif vRealize Orchestrator Appliance.

Conditions préalables

- Téléchargez et déployez le dispositif vRealize Orchestrator Appliance.
- Vérifiez que le dispositif vRealize Orchestrator Appliance est en cours d'exécution.

Procédure

1. Connectez-vous à la ligne de commande du dispositif vRealize Orchestrator Appliance en tant qu'utilisateur **racine**.
2. Pour activer l'accès SSH, exécutez la commande `/usr/bin/toggle-ssh enable`.
3. Pour désactiver l'accès SSH, exécutez la commande `/usr/bin/toggle-ssh disable`.

Configuration initiale

5

Avant de commencer à automatiser des tâches et à gérer des systèmes et des applications avec vRealize Orchestrator, vous devez utiliser le centre de contrôle vRealize Orchestrator pour configurer un fournisseur d'authentification externe. Vous pouvez également utiliser le centre de contrôle vRealize Orchestrator pour des tâches de configuration supplémentaires, telles que la gestion des licences et des informations de certificat, l'installation de plug-ins ou la surveillance de l'état de votre cluster vRealize Orchestrator.

Ce chapitre contient les rubriques suivantes :

Configuration d'un serveur vRealize Orchestrator autonome

Bien que vRealize Orchestrator Appliance soit une machine virtuelle basée sur une machine virtuelle basée sur Photon préconfigurée, vous devez configurer un fournisseur d'authentification avant d'accéder à toutes les fonctionnalités du centre de contrôle vRealize Orchestrator et de vRealize Orchestrator Client.

Configurer un serveur vRealize Orchestrator autonome avec l'authentification vRealize Automation

Pour préparer le dispositif vRealize Orchestrator Appliance, vous devez configurer les paramètres de l'hôte et le fournisseur d'authentification. Vous pouvez configurer vRealize Orchestrator pour l'authentification avec vRealize Automation. Utilisez l'authentification vRealize Automation avec vRealize Automation 8.x.

Conditions préalables

- Téléchargez et déployez la dernière version du dispositif vRealize Orchestrator Appliance. Reportez-vous à Télécharger et déployer le dispositif vRealize Orchestrator Appliance.
- Installez et configurez vRealize Automation 8.x, puis vérifiez que votre serveur vRealize Automation est en cours d'exécution. Consultez la documentation de vRealize Automation.

  Important La version de produit du fournisseur d'authentification vRealize Automation doit correspondre à celle de votre déploiement vRealize Orchestrator. Par exemple, pour authentifier un déploiement vRealize Orchestrator 8.7, vous devez utiliser un déploiement vRealize Automation 8.7.

Si vous prévoyez de créer un cluster :

- Configurez un équilibrage de charge pour distribuer le trafic entre plusieurs instances de vRealize Orchestrator. Consultez le Guide de l'équilibrage de charge VMware vRealize Orchestrator 8.x.

Procédure

1. Accédez au centre de contrôle pour démarrer l'assistant de configuration.
   a. Accédez à https://*your_orchestrator_FQDN*/vco-controlcenter.
   b. Connectez-vous en tant qu'utilisateur **racine** avec le mot de passe que vous avez entré lors du déploiement OVA.
2. Configurez le fournisseur d'authentification.
   a. Sur la page **Configurer le fournisseur d'authentification**, sélectionnez **vRealize Automation** dans le menu déroulant **Mode d'authentification**.
   b. Dans la zone de texte **Adresse d'hôte**, entrez l'adresse de votre hôte vRealize Automation et cliquez sur **SE CONNECTER**.

      Le format de l'adresse d'hôte vRealize Automation doit être https://*votre_nom_d'hôte_vra*.
   c. Cliquez sur **Accepter le certificat**.
   d. Entrez les informations d'identification du propriétaire de l'organisation vRealize Automation avec lequel vRealize Orchestrator sera configuré. Cliquez sur **ENREGISTRER**.
   e. Cliquez sur **ENREGISTRER LES MODIFICATIONS**.

      Un message indique que votre configuration est correctement enregistrée.

Résultats

Vous avez terminé la configuration du serveur vRealize Orchestrator.

Étape suivante

- Vérifiez que **CSP** est le fournisseur de licence configuré sur la page **Attribution de licences**.

- Vérifiez que le nœud est configuré correctement sur la page **Valider la configuration**.

  Note Suite à la configuration du fournisseur d'authentification, le serveur vRealize Orchestrator redémarre automatiquement après 2 minutes. Une vérification de la configuration immédiatement après l'authentification peut renvoyer un état de configuration non valide.

Configurer un serveur vRealize Orchestrator autonome avec l'authentification vSphere

Vous enregistrez le serveur vRealize Orchestrator auprès d'un serveur vCenter Single Sign-On à l'aide du mode d'authentification vSphere. Utilisez l'authentification vCenter Single Sign-On avec vCenter Server 6.0 et versions ultérieures.

Conditions préalables

- Téléchargez et déployez la dernière version du dispositif vRealize Orchestrator Appliance. Reportez-vous à Télécharger et déployer le dispositif vRealize Orchestrator Appliance.
- Installez et configurez une instance de vCenter Server avec le serveur vCenter Single Sign-On en cours d'exécution. Consultez la documentation de vSphere.

Si vous prévoyez de créer un cluster :

- Configurez un équilibrage de charge pour distribuer le trafic entre plusieurs instances de vRealize Orchestrator. Consultez le Guide de l'équilibrage de charge VMware vRealize Orchestrator 8.x.

Procédure

1. Accédez au centre de contrôle pour démarrer l'assistant de configuration.
   a. Accédez à https://*your_orchestrator_FQDN*/vco-controlcenter.
   b. Connectez-vous en tant qu'utilisateur **racine** avec le mot de passe que vous avez entré lors du déploiement OVA.

2 Configurez le fournisseur d'authentification.

a Sur la page **Configurer le fournisseur d'authentification**, sélectionnez **vSphere** dans le menu déroulant **Mode d'authentification**.

b Dans la zone de texte **Adresse de l'hôte**, entrez le nom de domaine complet ou l'adresse IP de l'instance de Platform Services Controller qui contient le vCenter Single Sign-On, puis cliquez sur **Se connecter**.

Note Si vous utilisez une instance externe de Platform Services Controller ou plusieurs instances de Platform Services Controller derrière un équilibrage de charge, vous devez manuellement importer les certificats de toutes les instances de Platform Services Controller qui partagent un domaine vCenter Single Sign-On.

Note Pour intégrer un vSphere Client différent à votre environnement vRealize Orchestrator configuré, vous devez configurer vSphere pour qu'il utilise les mêmes instances de Platform Services Controller enregistrées dans vRealize Orchestrator. Pour les environnements vRealize Orchestrator haute disponibilité, vous devez répliquer les instances de PCS derrière le serveur d'équilibrage de charge vRealize Orchestrator.

c Passez en revue les informations de certificat du fournisseur d'authentification et cliquez sur **Accepter le certificat**.

d Entrez les informations d'identification du compte d'administrateur local pour le domaine vCenter Single Sign-On. Cliquez sur **ENREGISTRER**.

Par défaut, ce compte est **`administrator@vsphere.local`** et le nom du locataire est **`vsphere.local`**.

e Dans la zone de texte **Groupe admin**, entrez le nom d'un groupe d'administrateurs et cliquez sur **RECHERCHER**.

Par exemple, **`vsphere.local\vcoadmins`**

f Sélectionnez le groupe d'administration à utiliser.

g Cliquez sur **ENREGISTRER LES MODIFICATIONS**.

Un message indique que votre configuration est correctement enregistrée.

Résultats

Vous avez terminé la configuration du serveur vRealize Orchestrator.

Étape suivante

- Vérifiez que **CIS** est le fournisseur de licence configuré sur la page **Attribution de licences**.

- Vérifiez que le nœud est configuré correctement sur la page **Valider la configuration**.

  Note Suite à la configuration du fournisseur d'authentification, le serveur vRealize Orchestrator redémarre automatiquement après 2 minutes. Une vérification de la configuration immédiatement après l'authentification peut renvoyer un état de configuration non valide.

Activation des fonctionnalités de vRealize Orchestrator avec les licences

L'accès à certaines fonctionnalités de vRealize Orchestrator est basé sur la licence appliquée à votre déploiement vRealize Orchestrator.

Après l'authentification, une licence est attribuée à l'instance de vRealize Orchestrator selon ce fournisseur d'authentification. Les licences contrôlent l'accès aux fonctionnalités de vRealize Orchestrator suivantes :

- Intégration Git
- Gestion des rôles
- Prise en charge multilingue (Python, Node.js et PowerShell)

Vous pouvez modifier manuellement la licence du serveur vRealize Orchestrator depuis la page **Licences** du centre de contrôle.

Note Il n'y a pas de limite quant au nombre de déploiements de vRealize Orchestrator auxquels vous pouvez appliquer la même licence, quel que soit le type de licence. Pour les licences vRealize Automation, il n'est pas nécessaire de disposer d'un environnement vRealize Automation déployé et configuré.

Authentification	Licence	Intégration Git	Gestion des rôles	Prise en charge multilingue
vSphere	vSphere vCloud Suite Standard	Non	Non	Non
vSphere	vRealize Automation vRealize Suite Advanced ou Enterprise vCloud Suite Advanced ou Enterprise	Oui	Oui	Oui
vRealize Automation	vRealize Automation vRealize Suite Advanced ou Enterprise vCloud Suite Advanced ou Enterprise	Oui	Les rôles sont gérés depuis l'instance de vRealize Automation utilisée pour l'authentification de vRealize Orchestrator.	Oui

Note Les licences standard de vRealize Suite n'incluent pas vRealize Automation ; elles ne prennent donc pas en charge l'accès aux fonctionnalités de vRealize Orchestrator.

Connexion à la base de données vRealize Orchestrator

Le serveur vRealize Orchestrator requiert une base de données pour le stockage des données.

Le dispositif vRealize Orchestrator Appliance déployé inclut une base de données PostgreSQL préconfigurée qui est utilisée par le serveur vRealize Orchestrator pour stocker des données.

La base de données postgreSQL n'est pas accessible aux utilisateurs.

Gérer les certificats

Émis pour un serveur en particulier et renfermant des informations sur la clé publique du serveur, le certificat vous autorise à signer tous les éléments créés dans vRealize Orchestrator et à en garantir l'authenticité. Lorsque le client reçoit un élément de votre serveur, le plus souvent un module, il vérifie votre identité et décide si oui ou votre signature est digne de confiance.

- Gérer les certificats vRealize Orchestrator

  Vous pouvez gérer les certificats vRealize Orchestrator depuis la page **Certificats** du centre de contrôle vRealize Orchestrator ou via vRealize Orchestrator Client, en utilisant les workflows contenant la balise *ssl_ trust_ manager*.

Gérer les certificats vRealize Orchestrator

Vous pouvez gérer les certificats vRealize Orchestrator depuis la page **Certificats** du centre de contrôle vRealize Orchestrator ou via vRealize Orchestrator Client, en utilisant les workflows contenant la balise *ssl_trust_manager*.

Importer un certificat dans un magasin de confiance d'Orchestrator

Le centre de contrôle vRealize Orchestrator utilise une connexion sécurisée pour communiquer avec vCenter Server, un système de gestion de base de données relationnelle (RDBMS), LDAP, Single Sign-On et d'autres serveurs. Vous pouvez importer le certificat TLS requis d'une URL ou d'un fichier codé PEM. Chaque fois que vous utilisez une connexion TLS à une instance de serveur, vous devez importer le certificat correspondant depuis l'onglet **Certificats de confiance** de la page **Certificats** et importer le certificat TLS correspondant.

Vous pouvez charger le certificat TLS dans vRealize Orchestrator à partir d'une adresse URL ou d'un fichier codé PEM.

Option	Description
Importer à partir de l'URL ou de l'URL du proxy	URL du serveur distant : `https://adresse_IP_de_votre_serveur` ou `adresse_IP_de_votre_serveur:port`
Importer à partir d'un fichier	Chemin d'accès au fichier de certificat codé PEM. **Note** Vous pouvez également importer un certificat de confiance en exécutant le workflow **Importer un certificat de confiance à partir d'un fichier** dans le vRealize Orchestrator Client. Le fichier importé via ce workflow doit être codé DER.

Pour plus d'informations sur l'importation d'un certificat, reportez-vous à Importer un certificat approuvée avec le centre de contrôle.

Certificat de signature de module

Les modules exportés à partir d'un serveur vRealize Orchestrator sont signés de manière numérique. Importez un certificat, exportez-le ou générez-en un nouveau pour la signature des modules. Les certificats de signature de module sont une forme d'identification numérique utilisée pour garantir la communication chiffrée et une signature pour vos modules Orchestrator.

Le dispositif vRealize Orchestrator Appliance inclut un certificat de signature de module généré automatiquement, basé sur les paramètres réseau du dispositif. Si les paramètres réseau du dispositif sont modifiés, vous devez générer manuellement un nouveau certificat de signature de module. Après avoir généré un nouveau certificat de signature de module, tous les modules exportés ultérieurement sont signés avec le nouveau certificat.

Générer un certificat TLS personnalisé pour vRealize Orchestrator

Vous pouvez utiliser vRealize Orchestrator Appliance pour générer un nouveau certificat TLS pour votre environnement ou définir un certificat personnalisé existant.

Le dispositif vRealize Orchestrator Appliance inclut un certificat TLS (Trusted Layer Security) généré automatiquement, basé sur les paramètres réseau du dispositif. Si les paramètres réseau du dispositif sont modifiés, vous devez générer manuellement un nouveau certificat. Vous pouvez créer une chaîne de certificats pour garantir une communication chiffrée et fournir une signature pour vos modules. Toutefois, le destinataire ne peut pas être sûr que le module auto-signé soit en fait un module créé par votre serveur et non par une partie tierce utilisant votre identité. Pour prouver l'identité de votre serveur, utilisez un certificat signé par une autorité de certification.

vRealize Orchestrator génère un certificat de serveur unique pour votre environnement. La clé privée est stockée dans la table `vmo_keystore` de la base de données vRealize Orchestrator.

Note Pour configurer votre dispositif vRealize Orchestrator Appliance afin qu'il utilise un certificat TLS personnalisé existant, reportez-vous à Définir un certificat TLS personnalisé pour vRealize Orchestrator.

Conditions préalables

Vérifiez que l'accès SSH pour le dispositif vRealize Orchestrator Appliance est activé. Reportez-vous à Activer ou désactiver l'accès SSH au dispositif vRealize Orchestrator Appliance.

Procédure

1. Connectez-vous à la ligne de commande de vRealize Orchestrator Appliance sur SSH en tant qu'utilisateur **racine**.
2. Exécutez la commande `vracli certificate ingress --generate auto --set stdin`.
3. Pour appliquer le certificat personnalisé à votre dispositif vRealize Orchestrator Appliance, exécutez le script de déploiement.
   a. Accédez au répertoire `/opt/scripts/`.

   ```
   cd /opt/scripts/
   ```

   b. Exécutez le script `./deploy.sh`.

   Important N'interrompez pas le script de déploiement. Le message suivant s'affiche à la fin de l'exécution du script :

   ```
   Prelude a été correctement déployé. Pour y accéder, accédez à
   adresse_de_votre_orchestrator
   ```

Étape suivante

Pour confirmer que la nouvelle chaîne de certificats est appliquée, exécutez la commande `vracli certificate ingress --list`.

Définir un certificat TLS personnalisé pour vRealize Orchestrator

Définissez un certificat TLS personnalisé pour votre dispositif vRealize Orchestrator Appliance.

Le dispositif vRealize Orchestrator Appliance inclut un certificat TLS (Trusted Layer Security) généré automatiquement, basé sur les paramètres réseau du dispositif.

Vous pouvez configurer votre dispositif vRealize Orchestrator Appliance pour qu'il utilise un certificat TLS personnalisé existant. Vous pouvez définir le certificat en important le fichier PEM pertinent de votre machine locale dans le dispositif vRealize Orchestrator Appliance. Vous pouvez également définir votre certificat TLS personnalisé en copiant la chaîne de certificats directement dans le dispositif vRealize Orchestrator Appliance. Les deux procédures nécessitent que vous exécutiez le script `.dans le script /deploy.sh`, avant que le nouveau certificat TLS puisse être utilisé dans votre déploiement vRealize Orchestrator.

Pour plus d'informations sur la génération d'un nouveau certificat TLS personnalisé, consultez Générer un certificat TLS personnalisé pour vRealize Orchestrator.

Conditions préalables

- Vérifiez que l'accès SSH pour le dispositif vRealize Orchestrator Appliance est activé. Reportez-vous à Activer ou désactiver l'accès SSH au dispositif vRealize Orchestrator Appliance.
- Vérifiez que le fichier PEM contenant le certificat TLS contient les composants suivants dans l'ordre défini :
  a La clé privée du certificat.
  b Le certificat principal.
  c Le cas échéant, le ou les certificats intermédiaires de l'autorité de certification.
  d Un certificat d'autorité de certification racine.

  Par exemple, la structure du certificat TLS peut être la suivante :

```
 -----BEGIN RSA PRIVATE KEY-----
<Private Key>
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
<Primary TLS certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root CA certificate>
-----END CERTIFICATE-----
```

Procédure

1 Définissez le certificat en important le fichier PEM dans le dispositif vRealize Orchestrator Appliance.

   a Importez le fichier PEM du certificat à partir de votre machine locale en exécutant une commande secure copy (SCP) à partir d'un shell SSH.

   Pour Linux, vous pouvez utiliser une commande SCP de terminal :

   ```
   scp ~/PEM_local_filepath/your_cert_file.PEM root@orchestrator_FQDN_or_IP:/
   PEM_orchestrator_filepath/your_cert_file.PEM
   ```

   Pour Windows, vous pouvez utiliser une commande PSCP du client PuTTY :

   ```
   pscp C:\PEM_local_filepath\your_cert_file.PEM root@<orchestrator_FQDN_or_IP>:/
   PEM_orchestrator_filepath/your_cert_file.PEM
   ```

   b Connectez-vous à la ligne de commande de vRealize Orchestrator Appliance sur SSH en tant qu'utilisateur **racine**.

   c Exécutez la commande `vracli certificate ingress --set` *your_cert_file.PEM*.

2 (Facultatif) Définissez le certificat en copiant la chaîne de certificats directement dans le dispositif.

   a Connectez-vous à la ligne de commande de vRealize Orchestrator Appliance sur SSH en tant qu'utilisateur **racine**.

   b Exécutez la commande `vracli certificate ingress --set stdin`.

   c Copiez et collez la chaîne de certificats, et appuyez sur Ctrl + D.

3 Pour appliquer le nouveau certificat TLS, exécutez le script de déploiement.

   a Accédez au répertoire `/opt/scripts/`.

   ```
   cd /opt/scripts/
   ```

   b Exécutez le script `./deploy.sh`.

   Important N'interrompez pas le script de déploiement. Le message suivant s'affiche à la fin de l'exécution du script :

   ```
   Prelude a été correctement déployé. Pour y accéder, accédez à https://
   your_orchestrator_FQDN.
   ```

Résultats

Vous avez défini un certificat TLS personnalisé pour votre dispositif vRealize Orchestrator Appliance.

Étape suivante

Pour confirmer que la nouvelle chaîne de certificats est appliquée, exécutez la commande `vracli certificate ingress --list`.

Importer un certificat approuvée avec le centre de contrôle

Pour communiquer en toute sécurité avec les autres serveurs, le serveur vRealize Orchestrator doit pouvoir vérifier leur identité. Pour cela, vous devrez peut-être importer le certificat TLS de l'entité distante dans le magasin de confiance de vRealize Orchestrator. Pour approuver un certificat, vous pouvez l'importer dans le magasin de confiance en établissant une connexion vers une URL spécifique ou l'importer directement en tant qu'un fichier codé PEM.

Procédure

1. Connectez-vous au centre de contrôle en tant qu'utilisateur **`racine`**.
2. Accédez à la page **Certificats**.
3. Sélectionnez **Certificats approuvés** et cliquez sur **Importer**.
4. Pour importer le certificat à partir d'un fichier, sélectionnez **Importer à partir d'un fichier codé PEM**.
5. Accédez au fichier de certificat et cliquez sur **Importer**.
6. Pour importer le certificat à partir d'une adresse URL, sélectionnez **Importer à partir d'une URL**.
7. Entrez l'adresse URL où votre certificat est stocké et cliquez sur **Importer**.

Résultats

Vous avez importé un certificat de serveur distant dans le magasin de confiance de vRealize Orchestrator.

Configuration des plug-ins vRealize Orchestrator

Le dispositif vRealize Orchestrator Appliance fournit un accès à une bibliothèque préinstallée de plug-ins par défaut. Les plug-ins vRealize Orchestrator par défaut sont configurés avec des workflows spécifiques des plug-ins exécutés dans vRealize Orchestrator Client.

Les plug-ins vRealize Orchestrator par défaut sont intégrés aux workflows de configuration. Vous pouvez exécuter ces workflows à partir de vRealize Orchestrator Client pour enregistrer les points de terminaison à des fins de gestion.

Les workflows de configuration comportent la balise *configuration*. Par exemple, pour accéder aux workflows utilisés pour gérer les brokers AMQP et les abonnements, entrez les balises *AMQP* et *Configuration* dans la zone de texte de recherche de la bibliothèque de workflows.

Gérer les plug-ins de vRealize Orchestrator

Sur la page **Gérer les plug-ins** du Centre de contrôle vRealize Orchestrator, vous pouvez afficher une liste de tous les plug-ins installés dans vRealize Orchestrator et procéder à des opérations de gestion de base.

Installer ou mettre à niveau un plug-in

Les plug-ins vRealize Orchestrator permettent au serveur vRealize Orchestrator de s'intégrer à d'autres produits logiciels. vRealize Orchestrator est fourni avec un ensemble de plug-ins par défaut préinstallés. Vous pouvez également étendre les capacités de la plate-forme vRealize Orchestrator en installant des plug-ins personnalisés.

Vous pouvez installer ou mettre à niveau les plug-ins depuis la page **Gérer les plug-ins** de vRealize Orchestrator. L'extension de fichier qui peut être utilisée est `.vmoapp`.

Pour plus d'informations sur l'installation ou la mise à niveau des plug-ins vRealize Orchestrator, reportez-vous à Installer ou mettre à jour un plug-in vRealize Orchestrator.

Modifier le niveau de journalisation des plug-ins

Au lieu de modifier le niveau de journalisation pour vRealize Orchestrator, vous pouvez le modifier uniquement pour des plug-ins spécifiques.

Désactiver un plug-in

Vous pouvez désactiver un plug-in en désactivant l'option **Activer le plug-in** en regard du nom du plug-in.

Cette action ne supprime pas le fichier du plug-in. Pour plus d'informations sur la désinstallation d'un plug-in dans vRealize Orchestrator, reportez-vous à Supprimer un plug-in.

Installer ou mettre à jour un plug-in vRealize Orchestrator

Vous pouvez installer ou mettre à jour des plug-ins tiers dans le centre de contrôle vRealize Orchestrator.

Conditions préalables

Téléchargez le fichier *.dar* ou *.vmoapp* du plug-in.

Note Le format de fichier recommandé pour les plug-ins vRealize Orchestrator est *.vmoapp*.

Procédure

1. Connectez-vous au centre de contrôle en tant qu'utilisateur **racine**.
2. Sélectionnez la page **Gérer les plug-ins**.
3. Cliquez sur **Parcourir** et sélectionnez le fichier *.dar* ou *.vmoapp* du plug-in à installer ou mettre à jour.
4. Cliquez sur **Télécharger**.

5 Vérifiez les informations du plug-in, le cas échéant acceptez le contrat de licence d'utilisateur final et cliquez sur **Installer**.

Le plug-in est installé ou mis à jour et le service du serveur vRealize Orchestrator est redémarré.

Étape suivante

Vérifiez que les informations du plug-in sont correctement répertoriées sur la page **Gérer les plug-ins**.

Supprimer un plug-in

Vous pouvez supprimer des plug-ins tiers du dispositif vRealize Orchestrator Appliance dans le centre de contrôle.

Note À partir de vRealize Orchestrator 8.0, vous ne supprimez plus manuellement le module du plug-in de vRealize Orchestrator Client.

Procédure

1 Connectez-vous au centre de contrôle en tant qu'utilisateur **racine**.

2 Sélectionnez **Gérer les plug-ins**.

3 Trouvez le plug-in que vous souhaitez supprimer, puis cliquez sur l'icône Supprimer ( ).

4 Confirmez que vous souhaitez supprimer le plug-in, puis cliquez sur **Supprimer**.

Résultats

Vous avez supprimé le plug-in du dispositif vRealize Orchestrator Appliance.

vRealize Orchestrator High Availability

Pour augmenter la disponibilité des services vRealize Orchestrator, démarrez plusieurs instances de serveur vRealize Orchestrator dans un cluster possédant une base de données partagée. vRealize Orchestrator fonctionne comme une instance unique jusqu'à ce qu'il soit configuré pour fonctionner comme partie d'un cluster.

Les instances de serveur vRealize Orchestrator qui possèdent des configurations de serveur et de plug-ins identiques fonctionnent ensemble dans un cluster et partagent une base de données.

Toutes les instances de serveur vRealize Orchestrator communiquent entre elles en échangeant des pulsations. Chaque pulsation est un horodatage que le nœud écrit dans la base de données partagée du cluster à certains intervalles de temps. Des problèmes de réseau, un serveur de base de données qui ne répond pas, ou une surcharge peuvent être à l'origine d'un nœud de cluster vRealize Orchestrator qui cesse de répondre. Si une instance de serveur vRealize Orchestrator ne parvient pas à envoyer des pulsations dans le délai d'expiration de basculement, elle est

considérée comme non réactive. Le délai d'expiration de basculement est égal à la valeur de l'intervalle de pulsation multiplié par le nombre de pulsations de basculement. Il sert à définir un nœud peu fiable et peut être personnalisé en fonction des ressources disponibles et de la charge de production.

Un nœud vRealize Orchestrator entre en mode veille lorsqu'il perd la connexion à la base de données et reste dans ce mode jusqu'à ce que la connexion à la base de données soit restaurée. Les autres nœuds du cluster prennent le contrôle du travail actif, en reprenant tous les workflows interrompus à partir de leurs derniers éléments inachevés, tels que des tâches pouvant contenir des scripts ou des appels de workflows.

Vous pouvez surveiller l'état de votre cluster vRealize Orchestrator à partir de l'onglet **Système** du tableau de bord vRealize Orchestrator Client. Pour configurer le signal de pulsation du cluster, le nombre de signaux de pulsation de basculement et le nombre de nœuds actifs, accédez à la page **Gestion du cluster Orchestrator** du centre de contrôle vRealize Orchestrator.

Valeurs maximales d'évolutivité de vRealize Orchestrator

Le tableau des limites d'évolutivité décrit les valeurs maximales recommandées pour les déploiements de vRealize Orchestrator 8.x.

Composant	Cibles d'échelle	Plus d'informations
Machines virtuelles	35 000	
Connexions à l'instance de vCenter Server	10	Voir Configuration de vCenter Server
Les nodes actifs dans un cluster	3	Voir Configurer un cluster vRealize Orchestrator
Workflows exécutés simultanément	300 par nœud	Voir Configuration des propriétés d'exécution de workflow
Workflows en cours d'exécution mis en file d'attente	10 000 par nœud	
Exécutions de workflow conservées	100 par nœud	
Jours d'expiration des événements du journal	15	

Configurer un cluster vRealize Orchestrator

Vous pouvez configurer votre nouveau déploiement de vRealize Orchestrator pour qu'il s'exécute en haute disponibilité en déployant trois nœuds et en les connectant en tant que cluster.

Un cluster vRealize Orchestrator se compose de trois instances de vRealize Orchestrator qui partagent une base de données PostgreSQL commune. La base de données du cluster vRealize Orchestrator configuré peut uniquement s'exécuter en mode asynchrone.

Pour créer un cluster vRealize Orchestrator, vous devez sélectionner une instance de vRealize Orchestrator comme nœud principal du cluster. Après avoir configuré le nœud principal, vous joignez les nœuds secondaires à celui-ci.

Le cluster vRealize Orchestrator créé est préconfiguré avec le basculement automatique.

Note L'échec du basculement automatique peut entraîner la perte des données de base de données.

Conditions préalables

- Téléchargez et déployez trois instances autonomes de vRealize Orchestrator. Reportez-vous à Télécharger et déployer le dispositif vRealize Orchestrator Appliance.

  Note Le nombre recommandé de nœuds pouvant être utilisés pour créer un environnement de vRealize Orchestrator mis en cluster est trois.

- Vérifiez que l'accès SSH est activé pour tous les nœuds vRealize Orchestrator. Reportez-vous à Activer ou désactiver l'accès SSH au dispositif vRealize Orchestrator Appliance.
- Configurez un serveur d'équilibrage de charge. Consultez le Guide de l'équilibrage de charge VMware vRealize Orchestrator 8.x.

Procédure

1 Configurez le nœud principal.

   a Connectez-vous à la ligne de commande vRealize Orchestrator Appliance du nœud principal sur SSH en tant qu'utilisateur **racine**.

   b Pour configurer le serveur d'équilibrage de charge du cluster, exécutez la commande `vracli load-balancer set`*load_balancer_FQDN*.

   c Connectez-vous au centre de contrôle du nœud principal et sélectionnez **Paramètres d'hôte**.

   d Cliquez sur **Modifier** et définissez l'adresse de l'hôte du serveur d'équilibrage de charge connecté.

   e Configurez le fournisseur d'authentification. Reportez-vous à Configuration d'un serveur vRealize Orchestrator autonome.

2 Joignez les nœuds secondaires au nœud principal.

   a Connectez-vous à la ligne de commande vRealize Orchestrator Appliance du nœud secondaire sur SSH en tant qu'utilisateur **racine**.

   b Pour joindre le nœud secondaire au nœud principal, exécutez la commande `vracli cluster join`*primary_node_hostname_or_IP*.

   c Entrez le mot de passe racine du nœud principal.

   d Répétez la procédure pour un autre nœud secondaire.

3 (Facultatif) Si votre nœud principal utilise un certificat personnalisé, vous devez définir le certificat dans le dispositif ou générer un nouveau certificat. Reportez-vous à Générer un certificat TLS personnalisé pour vRealize Orchestrator.

Note Le fichier contenant la chaîne de certificats doit être codé au format PEM.

4 Terminez le déploiement du cluster.

a Connectez-vous à la ligne de commande vRealize Orchestrator Appliance du nœud principal sur SSH en tant qu'utilisateur **racine**.

b Pour confirmer que tous les nœuds sont dans un état prêt, exécutez la commande `kubectl -n prelude get nodes`.

c Exécutez le script `/opt/scripts/deploy.sh` et attendez la fin du déploiement.

Résultats

Vous avez créé un cluster vRealize Orchestrator. Après avoir créé le cluster, vous pouvez accéder à votre environnement vRealize Orchestrator uniquement à partir de l'adresse de nom de domaine complet de votre serveur d'équilibrage de charge.

Note Étant donné que vous pouvez uniquement accéder au centre de contrôle du cluster avec le mot de passe racine de l'équilibrage de charge, vous ne pouvez pas modifier la configuration d'un nœud de cluster s'il a un mot de passe racine différent. Pour modifier la configuration de ce nœud, supprimez-le de l'équilibrage de charge, modifiez la configuration dans le centre de contrôle et rajoutez le nœud à l'équilibrage de charge.

Étape suivante

Pour surveiller l'état du cluster vRealize Orchestrator, connectez-vous à vRealize Orchestrator Client et accédez à l'onglet **Système** du tableau de bord. Reportez-vous à Surveiller un cluster vRealize Orchestrator.

Suppression d'un nœud de cluster vRealize Orchestrator

Vous pouvez supprimer une instance de vRealize Orchestrator afin de pouvoir réduire la capacité de votre cluster.

Après la suppression d'un nœud de votre cluster vRealize Orchestrator, ce nœud ne fonctionnera plus. Si vous souhaitez réutiliser ce nœud, vous devez supprimer son dispositif vRealize Orchestrator Appliance de votre instance de vCenter Server et le redéployer. Reportez-vous à Télécharger et déployer le dispositif vRealize Orchestrator Appliance.

Conditions préalables

Créez un cluster vRealize Orchestrator. Reportez-vous à Configurer un cluster vRealize Orchestrator.

Procédure

1 Connectez-vous à la ligne de commande vRealize Orchestrator Appliance du nœud que vous souhaitez supprimer en tant qu'utilisateur **racine**.

2 Pour supprimer le nœud de votre instance de vRealize Orchestrator, exécutez la commande `vracli cluster leave`.

3 Connectez-vous à la ligne de commande vRealize Orchestrator Appliance de l'un des nœuds restants en tant qu'utilisateur **racine**.

4 Exécutez la commande `kubectl -n prelude get nodes` et vérifiez que le nœud supprimé ne fait plus partie du cluster.

Monter en charge un déploiement autonome de vRealize Orchestrator

Vous pouvez augmenter la disponibilité et l'évolutivité de votre déploiement vRealize Orchestrator configuré en le faisant monter en charge.

Conditions préalables

- Téléchargez, déployez et configurez une instance de vRealize Orchestrator. Reportez-vous à Télécharger et déployer le dispositif vRealize Orchestrator Appliance et à Configuration d'un serveur vRealize Orchestrator autonome.
- Téléchargez et déployez deux instances supplémentaires de vRealize Orchestrator. Reportez-vous à Télécharger et déployer le dispositif vRealize Orchestrator Appliance.
- Configurez un serveur d'équilibrage de charge. Consultez le Guide de l'équilibrage de charge VMware vRealize Orchestrator 8.x.

Procédure

1 Configurez le nœud principal.

   a Connectez-vous au centre de contrôle de votre déploiement vRealize Orchestrator configuré en tant qu'utilisateur **racine**.

   b Sélectionnez **Configurer le fournisseur d'authentification** et annulez l'enregistrement de votre fournisseur d'authentification.

   c Sélectionnez **Paramètres d'hôte** et entrez le nom d'hôte du serveur d'équilibrage de charge.

   d Sélectionnez **Configurer le fournisseur d'authentification** et enregistrez à nouveau votre fournisseur d'authentification.

   e Connectez-vous à la ligne de commande de vRealize Orchestrator Appliance de l'instance configurée en tant qu'utilisateur **racine**.

   f Pour arrêter tous les services de l'instance de vRealize Orchestrator, exécutez la commande `/opt/scripts/deploy.sh --onlyClean`.

g Pour définir l'équilibrage de charge, exécutez `vracli load-balancer set` *load_balancer_FQDN*.

h (Facultatif) Si votre instance de vRealize Orchestrator utilise un certificat personnalisé, exécutez la commande `vracli certificate ingress --set` *your_cert_file.pem*.

Note Le fichier contenant la chaîne de certificats doit être codé au format PEM.

2 Joignez les nœuds secondaires à l'instance configurée.

a Connectez-vous à la ligne de commande vRealize Orchestrator Appliance du nœud secondaire en tant qu'utilisateur **racine**.

b Pour joindre le nœud secondaire à l'instance configurée, exécutez la commande `vracli cluster join`*primary_node_hostname_or_IP*.

c Répétez l'opération pour l'autre nœud secondaire.

3 Terminez le processus de montée en charge.

a Connectez-vous à la ligne de commande de vRealize Orchestrator Appliance de l'instance configurée en tant qu'utilisateur **racine**.

b Exécutez `/opt/scripts/deploy.sh` et attendez la fin du déploiement.

Résultats

Vous avez fait monté en charge votre déploiement de vRealize Orchestrator.

Surveiller un cluster vRealize Orchestrator

Vous pouvez surveiller votre cluster vRealize Orchestrator existant via l'onglet **Système** du tableau de bord vRealize Orchestrator Client.

La méthode recommandée pour surveiller les états de synchronisation de la configuration des instances de vRealize Orchestrator se fait via l'onglet **Système** du tableau de bord vRealize Orchestrator Client.

Note Si vous ne parvenez pas à accéder au tableau de bord vRealize Orchestrator Client, vous pouvez également surveiller l'état de vos instances de vRealize Orchestrator en exécutant la commande `kubectl get pods -n prelude` à partir de la ligne de commande vRealize Orchestrator Appliance.

État de synchronisation de la configuration	Description
EN COURS D'EXÉCUTION	Le service vRealize Orchestrator est disponible et peut accepter des demandes.
VEILLE	Le service vRealize Orchestrator ne peut pas traiter les demandes parce que : ■ Le nœud fait partie d'un cluster Haute disponibilité et reste en mode veille jusqu'à ce que le nœud principal échoue. ■ Le service ne peut pas vérifier les prérequis de configuration (par exemple, une connexion valide à la base de données, au fournisseur d'authentification et à la licence de l'instance de vRealize Orchestrator).
Impossible de récupérer l'état d'intégrité du service	Le service du serveur vRealize Orchestrator ne peut pas être contacté, parce qu'il s'est arrêté ou parce qu'un problème réseau est survenu.
En attente de redémarrage	Le centre de contrôle détecte une modification de la configuration et le serveur vRealize Orchestrator redémarre automatiquement.

Configuration du programme d'amélioration du produit

Si vous décidez de participer au programme d'amélioration du produit, des informations anonymes sont envoyées à VMware dans le but d'améliorer la qualité, la fiabilité et la fonctionnalité des produits et des services de VMware.

Catégories d'informations envoyées à VMware

Le programme d'amélioration du produit (CEIP) fournit à VMware des informations nous permettant d'améliorer nos produits et services ainsi que de résoudre des problèmes.

Les détails concernant les données recueillies via le CEIP et les fins auxquelles elles sont utilisées par VMware sont définis dans le Centre d'approbation et d'assurance à l'adresse http://www.vmware.com/trustvmware/ceip.html. Pour rejoindre ou quitter le programme CEIP pour ce produit, reportez-vous à Rejoindre ou quitter le programme d'amélioration du produit.

Rejoindre ou quitter le programme d'amélioration du produit

Rejoignez le programme d'amélioration du produit à partir de la ligne de commande de vRealize Orchestrator Appliance.

Procédure

1. Connectez-vous à la ligne de commande du dispositif vRealize Orchestrator Appliance en tant qu'utilisateur **racine**.
2. Pour rejoindre le programme d'amélioration du produit, exécutez la commande `vracli ceip on`.

3 Vérifiez les informations du programme d'amélioration du produit et exécutez la commande `vracli ceip on --acknowledge-ceip`.

4 Redémarrez les services vRealize Orchestrator.

   a Pour redémarrer le service du serveur, exécutez la commande `kubectl -n prelude exec -it` *your_vro_pod* `-c vco-server-app /bin/bash`.

   b Pour arrêter le service, exécutez la commande `kill 1`.

   c Pour redémarrer le service du centre de contrôle, exécutez la commande `kubectl -n prelude exec -it` *your_vro_pod* `-c vco-controlcenter-app /bin/bash`.

   d Pour arrêter le service, exécutez la commande `kill 1`.

5 Pour quitter le programme d'amélioration du produit, exécutez la commande `vracli ceip off`.

6 Répétez les étapes de redémarrage des services.

Utilisation des services vRealize Orchestrator API

6

Vous pouvez configurer vRealize Orchestrator à l'aide du centre de contrôle, et également modifier les paramètres de configuration du serveur vRealize Orchestrator à l'aide de l'API REST de vRealize Orchestrator, de l'API REST du centre de contrôle ou de l'utilitaire de ligne de commande présent dans le dispositif.

Le plug-in de configuration est inclus par défaut dans le module vRealize Orchestrator. Vous pouvez accéder aux workflows de configuration de plug-in à partir de la bibliothèque de workflows de vRealize Orchestrator ou de l'API REST de vRealize Orchestrator. Ces workflows vous permettent de modifier les paramètres du certificat approuvé et du keystore du serveur vRealize Orchestrator. Pour plus d'informations sur tous les appels de services disponibles de l'API REST de vRealize Orchestrator, consultez la documentation *vRealize Orchestrator Server API*, disponible à l'adresse https://*your_orchestrator_FQDN*/vco/api/docs.

Gestion des certificats TLS et des keystores à l'aide de l'API REST

Outre la gestion des certificats TLS à l'aide du centre de contrôle, vous pouvez également gérer des certificats et des keystores approuvés lorsque vous exécutez des workflows à partir du plug-in de configuration ou à l'aide de l'API REST.

Le plug-in de configuration contient des workflows pour l'importation et la suppression des certificats TLS et des keystores. Vous pouvez accéder à ces workflows en choisissant **Bibliothèque > Workflows > SSL Trust Manager** et à **Bibliothèque > Workflows > Keystores** dans vRealize Orchestrator Client. Vous pouvez également exécuter ces workflows à l'aide de l'API REST vRealize Orchestrator.

L'API REST du centre de contrôle donne accès aux ressources pour configurer le serveur vRealize Orchestrator. Vous pouvez utiliser l'API REST du centre de contrôle avec des systèmes tiers pour automatiser la configuration de vRealize Orchestrator. Le point de terminaison racine de l'API REST du centre de contrôle est https://*your_orchestrator_FQDN*/vco/api. Pour plus d'informations sur tous les appels de service disponibles que vous pouvez effectuer à l'API REST du centre de contrôle, reportez-vous à la documentation de *vRealize Orchestrator Control Center API*, à l'adresse https://*your_orchestrator_FQDN*/vco-controlcenter/docs.

Supprimer un certificat TLS à l'aide de l'API REST

Vous pouvez supprimer un certificat TLS en exécutant le workflow Supprimer un certificat approuvé du plug-in Configuration ou à l'aide de l'API REST.

Procédure

1. Soumettez une demande `GET` au niveau de l'URL du service de workflow du workflow Supprimer un certificat approuvé .

   ```
   GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Delete trusted certificate
   ```

2. Récupérez la définition du workflow Supprimer un certificat approuvé en soumettant une demande `GET` au niveau de l'URL de la définition.

   ```
   GET https://{orchestrator_host}:{port}/vco/api/workflows/8a70a326-ffd7-4fef-97e0-2002ac49f5bd
   ```

3. Soumettez une demande `POST` au niveau de l'URL qui comporte les objets d'exécution du workflow Supprimer un certificat approuvé.

   ```
   POST https://{orchestrator_host}:{port}/vco/api/workflows/8a70a326-ffd7-4fef-97e0-2002ac49f5bd/executions/
   ```

4. Indiquez le nom du certificat que vous souhaitez supprimer en tant que paramètre d'entrée du workflow Supprimer un certificat approuvé dans un élément de contexte d'exécution du corps de la demande.

Importer des certificats TLS à l'aide de l'API REST

Vous pouvez importer des certificats TLS en exécutant le workflow à partir du plug-in de configuration ou à l'aide de l'API REST.

Vous pouvez importer un certificat approuvé à partir d'un fichier ou d'une URL. Voir Importer un certificat approuvée avec le centre de contrôle

Procédure

1 Soumettez une demande `GET` au niveau de l'URL du service de workflow.

Option	Description
Importer un certificat approuvé à partir d'un fichier	Permet d'importer un certificat approuvé à partir d'un fichier.
Importer un certificat approuvé à partir d'une URL	Permet d'importer un certificat approuvé à partir d'une URL.
Importer un certificat approuvé à l'aide d'un serveur proxy	Permet d'importer un certificat approuvé à partir d'une adresse URL à l'aide d'un serveur proxy.
Importer un certificat approuvé à partir d'une URL avec un alias de certificat	Permet d'importer un certificat approuvé avec un alias de certificat, à partir d'une adresse URL.

Pour importer un certificat approuvé à partir d'un fichier, soumettez la demande `GET` suivante :

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Import
               trusted certificate from a file
```

2 Récupérez la définition du workflow en soumettant une demande `GET` au niveau de l'URL de la définition.

Pour récupérer la définition du workflow Importer un certificat approuvé à partir d'un fichier, soumettez la demande `GET` suivante :

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/
93a7bb21-0255-4750-9293-2437abe9d2e5
```

3 Soumettez une demande `POST` au niveau de l'URL qui comporte les objets d'exécution du workflow.

Pour le workflow Importer un certificat approuvé à partir d'un fichier, soumettez la demande `POST` suivante :

```
POST https://{orchestrator_host}:{port}/vco/api/workflows/
93a7bb21-0255-4750-9293-2437abe9d2e5/executions
```

4 Veillez à indiquer les valeurs des paramètres d'entrée du workflow dans un élément de contexte d'exécution de la demande.

Paramètre	Description
cer	Le fichier CER à partir duquel vous souhaitez importer le certificat TLS. Ce paramètre s'applique au workflow Importer un certificat approuvé à partir d'un fichier.
url	L'URL à partir de laquelle vous souhaitez importer le certificat TLS. Pour les services autres que HTTPS, le format pris en charge est *adresse_IP_ou_nom_DNS:port*. Ce paramètre s'applique au workflow Importer un certificat approuvé à partir d'un fichier.

Créer un keystore à l'aide de l'API REST

Vous pouvez créer un keystore en exécutant le workflow Créer un keystore du plug-in de configuration ou à l'aide de l'API REST.

Procédure

1 Soumettez une demande `GET` au niveau de l'URL du service de workflow du workflow Créer un keystore

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Create a keystore
```

2 Récupérez la définition du workflow Créer un keystore en soumettant une demande `GET` au niveau de l'URL de la définition.

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/6c301bff-e8fe-4ae0-
ad08-5318178594b3/
```

3 Soumettez une demande `POST` au niveau de l'URL qui comporte les objets d'exécution du workflow Créer un keystore.

```
POST https://{orchestrator_host}:{port}/vco/api/workflows/6c301bff-e8fe-4ae0-
ad08-5318178594b3/executions/
```

4 Fournissez le nom du keystore que vous souhaitez créer en tant que paramètre d'entrée du workflow Créer un keystore dans un élément de contexte d'exécution dans la demande.

Supprimer un keystore à l'aide de l'API REST

Vous pouvez supprimer un keystore en exécutant le workflow Supprimer un keystore du plug-in de configuration ou à l'aide de l'API REST.

Procédure

1 Soumettez une demande `GET` au niveau de l'URL du service de workflow du workflow Supprimer un keystore.

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Delete a keystore
```

2 Récupérez la définition du workflow Supprimer un keystore en soumettant une demande `GET` au niveau de l'URL de la définition.

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/
7a3389eb-1fab-4d77-860b-81b66bb45b86/
```

3 Soumettez une demande `POST` au niveau de l'URL qui comporte les objets d'exécution du workflow Supprimer un keystore.

```
POST https://{orchestrator_host}:{port}/vco/api/workflows/
7a3389eb-1fab-4d77-860b-81b66bb45b86/executions/
```

4 Fournissez le keystore que vous souhaitez supprimer en tant que paramètre d'entrée du workflow du keystore dans un élément de contexte d'exécution dans la demande.

Ajouter une clé à l'aide de l'API REST

Vous pouvez ajouter une clé en exécutant le workflow Ajouter une clé du plug-in de configuration ou à l'aide de l'API REST.

Procédure

1 Soumettez une demande `GET` au niveau de l'URL du service de workflow du workflow Ajouter une clé.

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Add key
```

2 Récupérez la définition du workflow Ajouter une clé en soumettant une demande `GET` au niveau de l'URL de la définition.

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/6c301bff-e8fe-4ae0-
ad08-5318178594b3/
```

3 Soumettez une demande `POST` au niveau de l'URL qui comporte les objets d'exécution du workflow Ajouter une clé.

```
POST https://{orchestrator_host}:{port}/vco/api/workflows/6c301bff-e8fe-4ae0-
ad08-5318178594b3/executions/
```

4 Fournissez le keystore, l'alias de clé, la clé encodée PEM, la chaîne de certificat et le mot de passe de clé en tant que paramètres d'entrée du workflow Ajouter une clé dans un élément de contexte d'exécution dans la demande.

Autres options de configuration 7

Vous pouvez utiliser le centre de contrôle pour modifier le comportement par défaut de vRealize Orchestrator.

Ce chapitre contient les rubriques suivantes :

Reconfiguration de l'authentification

Une fois que vous configurez la méthode d'authentification lors de la configuration initiale du centre de contrôle, vous pouvez modifier le fournisseur d'authentification ou les paramètres configurés à tout moment.

Modifier le fournisseur d'authentification

Pour modifier le mode d'authentification ou les paramètres de connexion du fournisseur d'authentification, vous devez d'abord désinscrire le fournisseur d'authentification existant.

Procédure

1. Connectez-vous au centre de contrôle en tant qu'utilisateur **`racine`**.
2. Sur la page **Configurer le fournisseur d'authentification**, cliquez sur le bouton **DÉSINSCRIRE** en regard de la zone de texte Adresse d'hôte pour désinscrire le fournisseur d'authentification en cours d'utilisation.

Résultats

Vous avez désinscrit le fournisseur d'authentification.

Étape suivante

Reconfigurez l'authentification dans le centre de contrôle. Reportez-vous à Configuration d'un serveur vRealize Orchestrator autonome.

Modifier les paramètres d'authentification

Si vous utilisez vSphere comme fournisseur d'authentification dans le centre de contrôle, vous pouvez modifier le locataire par défaut du groupe d'administrateurs vRealize Orchestrator.

Conditions préalables

Configurez vSphere en tant que fournisseur d'authentification pour votre déploiement de vRealize Orchestrator. Reportez-vous à Configurer un serveur vRealize Orchestrator autonome avec l'authentification vSphere.

Note L'authentification vRealize Automation n'inclut pas ces paramètres.

Procédure

1. Connectez-vous au centre de contrôle en tant qu'utilisateur **racine**.
2. Sélectionnez **Configurer le fournisseur d'authentification**.
3. Cliquez sur le bouton **MODIFIER** en regard de la zone de texte **Locataire par défaut**.
4. Remplacez le nom du locataire.
5. Cliquez sur le bouton **MODIFIER** en regard de la zone de texte **Groupe admin**.

   Note Si vous ne reconfigurez pas le groupe d'administrateurs, il reste vide et vous ne pouvez plus accéder au centre de contrôle.
6. Entrez le nom d'un groupe d'administrateurs et cliquez sur **RECHERCHER**.
7. Sélectionnez un groupe d'administrateurs.
8. Modifiez le groupe d'administrateurs.
9. Pour terminer la modification des paramètres d'authentification, cliquez sur **ENREGISTRER LES MODIFICATIONS**.

Configuration des propriétés d'exécution de workflow

Par défaut, vous pouvez exécuter jusqu'à 300 workflows par nœud, et jusqu'à 10 000 workflows peuvent être mis en file d'attente si le nombre de workflows en cours d'exécution est dépassé.

Lorsque le nœud vRealize Orchestrator doit exécuter plus de 300 workflows simultanés, les exécutions de workflow en attente sont mises en file d'attente. Lorsqu'une exécution de workflow active est terminée, le workflow suivant dans la file d'attente commence à s'exécuter. Si le nombre maximal de workflows en file d'attente est atteint, les exécutions de workflow suivantes échouent jusqu'à ce que l'un des workflows en attente commence à s'exécuter.

Vous pouvez configurer les propriétés d'exécution du workflow sur la page **Options avancées** du centre de contrôle.

Option	Description
Activer le mode sans échec	Si le mode sans échec est activé, tous les workflows exécutés sont annulés et ne reprennent pas lors du prochain démarrage du nœud vRealize Orchestrator.
Nombre de workflows en cours d'exécution simultanée	Nombre de workflows qui s'exécutent simultanément. La valeur par défaut est de 300 workflows par nœud.
Quantité maximale de workflows en cours d'exécution dans la file d'attente	Nombre de demandes d'exécution de workflow accepté par le serveur vRealize Orchestrator avant son indisponibilité. La valeur par défaut est de 10 000 workflows par nœud.
Nombre maximal d'exécutions conservées par workflow	Nombre maximal d'exécutions de workflow terminées qui sont conservées dans l'historique par workflow. Dès que le nombre est dépassé, l'exécution la plus ancienne est supprimée. La valeur par défaut est de 100 opérations par workflow.
Jours d'expiration des événements du journal	Nombre de jours de veille des événements de journaux dans la base de données avant leur purge. La valeur par défaut est de 15 jours.

Fichiers journaux de vRealize Orchestrator

Le support technique de VMware demande systématiquement des informations de diagnostic lorsque vous envoyez une demande d'assistance. Ces informations de diagnostic contiennent des journaux spécifiques au produit et des fichiers de configuration de l'hôte sur lequel le produit s'exécute.

Les journaux du dispositif vRealize Orchestrator Appliance sont stockés dans le répertoire `/data/vco/usr/lib/vco/app-server/logs/`. Vous exportez les journaux de votre déploiement de vRealize Orchestrator Appliance en vous connectant à la ligne de commande du dispositif et en exécutant la commande `vracli log-bundle`. Le bundle de journaux généré est enregistré dans le dossier racine de votre dispositif vRealize Orchestrator Appliance.

Persistance de la journalisation

Vous pouvez consigner des informations dans n'importe quel type de script vRealize Orchestrator, par exemple, un workflow, une stratégie ou une action. Ces informations ont des types et des niveaux. Le type peut être persistant ou non persistant. Le niveau peut être `DEBUG`, `INFO`, `WARN`, `ERROR`, `TRACE` et `FATAL`.

Tableau 7-1. Création de journaux persistants et non persistants

Niveau de journal	Type Persistant	Type non-persistant
DEBUG	Server.debug("texte court", "texte long") ;	System.debug("texte")
INFO	Server.log("texte court", "texte long") ;	System.log ("texte") ;
WARN	Server.warn("texte court", "texte long") ;	System.warn ("texte");
ERROR	Server.error ("texte court", "texte long") ;	System.eror ("texte") ;

Journaux persistants

Les journaux persistants (journaux du serveur) assurent le suivi des journaux d'exécution de workflows précédents et sont stockés dans la base de données vRealize Orchestrator.

Journaux non persistants

Lorsque vous utilisez un journal non persistant (journal système) pour créer des scripts, le serveur vRealize Orchestrator notifie toutes les applications vRealize Orchestrator en cours d'exécution sur ce journal, mais ces informations ne sont pas stockées dans la base de données. Lorsque l'application est redémarrée, les informations de journalisation sont perdues. Les journaux non persistants sont utilisés à des fins de débogage et pour des informations en direct. Pour afficher les journaux système, vous devez sélectionner une exécution de workflow terminée dans vRealize Orchestrator Client et sélectionner l'onglet **Journaux**.

Configuration des journaux de vRealize Orchestrator

Sur la page **Configurer les journaux**, vous pouvez définir le niveau de journal de serveur et du journal de scripts dont vous avez besoin. Si l'un des journaux est généré plusieurs fois par jour, il devient difficile de déterminer l'origine des problèmes.

Le niveau de journal par défaut du journal de serveur et du journal de scripts est `INFO`. La modification du niveau de journal affecte tous les nouveaux messages que le serveur inscrit dans les journaux ainsi que le nombre de connexions actives à la base de données. La verbosité de la journalisation diminue en ordre décroissant.

Attention Définissez uniquement le niveau de journal sur `DÉBOGAGE` ou `TOUT` pour déboguer un problème. N'utilisez pas ces paramètres dans un environnement de production, car cela peut considérablement dégrader les performances.

Générer les journaux vRealize Orchestrator

Vous pouvez exporter les journaux de votre déploiement en vous connectant à la ligne de commande vRealize Orchestrator Appliance en tant qu'utilisateur **racine** et en exécutant la commande `vracli log-bundle`. Le bundle de journaux généré est stocké dans le dossier racine du dispositif.

.

Note Lorsqu'un cluster comprend plusieurs instances de vRealize Orchestrator, le bundle de journaux incluent les journaux de toutes les instances de vRealize Orchestrator dans le cluster.

Configurer l'intégration de la journalisation à vRealize Log Insight

Vous pouvez configurer vRealize Orchestrator pour envoyer vos informations de journalisation au serveur vRealize Log Insight.

Vous pouvez configurer une intégration de journalisation à un serveur vRealize Log Insight à l'aide de la ligne de commande vRealize Orchestrator Appliance.

Note Pour plus d'informations sur la configuration d'une intégration de journalisation à un serveur syslog distant, reportez-vous à la section Créer ou remplacer une intégration Syslog dans vRealize Orchestrator.

Conditions préalables

- Configurez votre serveur vRealize Log Insight. Consultez la *Documentation de vRealize Log Insight*.
- Vérifiez que votre version de vRealize Log Insight est 4.7.1 ou une version ultérieure.

Procédure

1. Connectez-vous à la ligne de commande du dispositif vRealize Orchestrator Appliance en tant qu'utilisateur **racine**.
2. Pour configurer l'intégration de la journalisation à vRealize Log Insight, exécutez la commande `vracli vrli set`*vRLI_FQDN*.

   Note Si votre instance de vRealize Orchestrator utilise un certificat auto-signé, vous pouvez désactiver l'authentification SSL en incluant l'argument facultatif `-k` ou `--insecure`.

Étape suivante

Pour plus d'informations sur les options de configuration de vRealize Log Insight, exécutez la commande `vracli vrli -h`.

Créer ou remplacer une intégration Syslog dans vRealize Orchestrator

Vous pouvez configurer vRealize Orchestrator pour envoyer vos informations de journalisation à un ou plusieurs serveurs syslog distants.

La commande `vracli remote-syslog set` est utilisée pour créer une intégration syslog ou remplacer les intégrations existantes.

L'intégration syslog vRealize Orchestrator distante prend en charge trois types de connexion :

- Sur UDP.
- Sur TCP sans TLS.

  Note Pour créer une intégration syslog sans utiliser TLS, ajoutez l'indicateur `--disable-ssl` à la commande `vracli remote-syslog set`.

- Sur TCP avec TLS.

Pour plus d'informations sur la configuration d'une intégration de journalisation avec vRealize Log Insight, reportez-vous à Configurer l'intégration de la journalisation à vRealize Log Insight.

Conditions préalables

Configurez un ou plusieurs serveurs syslog.

Procédure

1. Connectez-vous à la ligne de commande du dispositif vRealize Orchestrator Appliance en tant qu'utilisateur **racine**.
2. Pour créer une intégration à un serveur syslog, exécutez la commande `vracli remote-syslog set`.

   ```
   vracli remote-syslog set -id name_of_integration protocol_type://
   syslog_URL_or_FQDN:syslog_port
   ```

   Note Si vous n'entrez pas de port dans la commande `vracli remote-syslog set`, la valeur de port est définie par défaut sur 514.

   Note Vous pouvez ajouter un certificat à la configuration syslog. Pour ajouter un fichier de certificat, utilisez l'indicateur `--ca-file`. Pour ajouter un certificat en texte brut, utilisez l'indicateur `--ca-cert`.

3. (Facultatif) Pour remplacer une intégration syslog existante, exécutez `vracli remote-syslog set` et définissez la valeur de l'indicateur `-id` sur le nom de l'intégration que vous souhaitez remplacer.

   Note Par défaut, le dispositif vRealize Orchestrator Appliance demande de confirmer que vous souhaitez remplacer l'intégration de syslog. Pour ignorer la demande de confirmation, ajoutez l'indicateur `-f` ou `--force` à la commande `vracli remote-syslog set`.

Étape suivante

Pour consulter les intégrations syslog actuelles dans le dispositif, exécutez la commande `vracli remote-syslog`.

Supprimer une intégration Syslog dans vRealize Orchestrator

Vous pouvez supprimer des intégrations syslog depuis votre instance de vRealize Orchestrator Appliance en exécutant la commande `vracli remote-syslog unset`.

Conditions préalables

Créez une ou plusieurs intégrations syslog dans le dispositif vRealize Orchestrator Appliance. Reportez-vous à Créer ou remplacer une intégration Syslog dans vRealize Orchestrator.

Procédure

1. Connectez-vous à la ligne de commande du dispositif vRealize Orchestrator Appliance en tant qu'utilisateur **racine**.
2. Supprimez les intégrations syslog du dispositif vRealize Orchestrator Appliance.
   a. Pour supprimer une intégration syslog spécifique, exécutez la commande `vracli remote-syslog unset -id` *Integration_ name*.
   b. Pour supprimer toutes les intégrations syslog sur le dispositif vRealize Orchestrator Appliance, exécutez la commande `vracli remote-syslog unset` sans l'indicateur `-id`.

   Note Par défaut, le dispositif vRealize Orchestrator Appliance demande de confirmer que vous souhaitez supprimer toutes les intégrations syslog. Pour ignorer la demande de confirmation, ajoutez l'indicateur `-f` ou `--force` à la commande `vracli remote-syslog unset`.

Activer la journalisation de débogage Kerberos

Vous pouvez résoudre les problèmes de plug-in vRealize Orchestrator en modifiant le fichier de configuration Kerberos utilisé par le plug-in.

Le fichier de configuration Kerberos se trouve dans le répertoire `/data/vco/usr/lib/vco/app-server/conf/` du dispositif vRealize Orchestrator Appliance.

Procédure

1. Connectez-vous à la ligne de commande du dispositif vRealize Orchestrator Appliance en tant qu'utilisateur **racine**.
2. Exécutez la commande `kubectl -n prelude edit deployment vco-app`.
3. Dans le fichier de déploiement, localisez et modifiez la chaîne `-Djava.security.krb5.conf=/usr/lib/vco/app-server/conf/krb5.conf'`.

   ```
   -Djava.security.krb5.conf=/usr/lib/vco/app-server/conf/krb5.conf
   -Dsun.security.krb5.debug=true'
   ```

4. Enregistrez les modifications et quittez l'éditeur de fichiers.

5 Exécutez la commande `kubectl -n prelude get pods`.

Attendez que tous les espaces soient en cours d'exécution.

6 Vérifiez que la journalisation de débogage Kerberos soit activée.

```
kubectl -n prelude log {vco_app_name} -c vco-server-app | grep krb5
```

Vérifiez que les journaux contiennent un message similaire.

```
kubectl -n prelude log vco-app-5c965f9b9d-v8srd -c vco-server-app | grep krb5
12:23:05,417 INFO O11N:75 - Sysprop: java.security.krb5.conf = /usr/lib/vco/app-server/
conf/krb5.conf
12:23:05,421 INFO O11N:75 - Sysprop: sun.security.krb5.debug = true
2019-10-22 12:23:38.521+0000 [Thread-19] INFO {} [O11N] Sysprop: java.security.krb5.conf
= /usr/lib/vco/app-server/conf/krb5.conf
2019-10-22 12:23:38.525+0000 [Thread-19] INFO {} [O11N] Sysprop: sun.security.krb5.debug =
true
Java config name: /usr/lib/vco/app-server/conf/krb5.conf
EType: sun.security.krb5.internal.crypto.Aes256CtsHmacSha1EType
```

Activation des extensions Opentracing et Wavefront

Les extensions Opentracing et Wavefront pour vRealize Orchestrator fournissent des outils afin de collecter des données sur votre environnement vRealize Orchestrator. Vous pouvez utiliser ces données pour le dépannage du système vRealize Orchestrator et des workflows.

Avant de pouvoir configurer vRealize Orchestrator pour utiliser les extensions Opentracing et Wavefront, vous devez les activer dans le dispositif vRealize Orchestrator Appliance.

Conditions préalables

- Vérifiez que le service SSH du dispositif vRealize Orchestrator Appliance est activé. Reportez-vous à Activer ou désactiver l'accès SSH au dispositif vRealize Orchestrator Appliance.
- Si vous avez activé les versions précédentes des extensions Opentracing ou Wavefront, vous devez les supprimer avant d'activer la version actuelle. Par exemple, si vous avez précédemment activé la version 8.1.0 de l'extension Wavefront, vous devez exécuter la commande `rm /data/vco/usr/lib/vco/app-server/extensions/wavefront-8.1.0.jar`.

Procédure

1 Connectez-vous au dispositif vRealize Orchestrator Appliance sur SSH en tant que **racine**.

2 Pour répertorier toutes les extensions disponibles, exécutez la commande `ls /data/vco/usr/lib/vco/app-server/extensions/`.

3 Exécutez la commande suivante pour activer l'extension Opentracing.

```
mv /data/vco/usr/lib/vco/app-server/extensions/opentracing-8.7.0.jar.inactive /
data/vco/usr/lib/vco/app-server/extensions/opentracing-8.7.0.jar
```

4 Exécutez la commande suivante pour activer l'extension Wavefront.

```
mv /data/vco/usr/lib/vco/app-server/extensions/wavefront-8.7.0.jar.inactive /
data/vco/usr/lib/vco/app-server/extensions/wavefront-8.7.0.jar
```

5 Connectez-vous au centre de contrôle et confirmez que les extensions figurent sur la page **Propriétés de l'extension**.

Étape suivante

Configurez l'intégration de Opentracing et de Wavefront avec vRealize Orchestrator sur la page **Propriétés de l'extension**. Reportez-vous à Configurer l'extension Opentracing et à Configurez l'extension Wavefront..

Configurer l'extension Opentracing

L'extension Opentracing envoie des données sur les exécutions de workflow à un serveur Jaeger. Les données incluent l'état du workflow, les paramètres d'entrée et de sortie, l'utilisateur qui a initié l'exécution du workflow ainsi que les données de l'ID du workflow.

Conditions préalables

- Vérifiez que Opentracing est activé dans le dispositif vRealize Orchestrator Appliance. Reportez-vous à Activation des extensions Opentracing et Wavefront.
- Déployez un serveur Jaeger pour l'utiliser dans l'extension Opentracing. Pour en savoir plus, reportez-vous à Démarrage avec la documentation Jaeger.

Procédure

1 Connectez-vous au centre de contrôle en tant qu'utilisateur **racine**.

2 Sélectionnez la page **Propriétés de l'extension**.

3 Sélectionnez l'extension Opentracing.

4 Entrez l'adresse et le port hôte du serveur Jaeger.

Note Insérez deux barres obliques (« // ») avant d'entrer l'adresse du serveur.

5 Cliquez sur **Enregistrer**.

Résultats

Vous avez configuré l'extension Opentracing pour vRealize Orchestrator.

Étape suivante

- Pour accéder à l'interface utilisateur Jaeger contenant les données collectées par l'extension Opentracing, accédez à l'adresse de l'hôte entrée lors de la configuration.
- Sous l'option **Service**, sélectionnez **Workflows**.
- Pour spécifier les données à afficher, utilisez l'option **Balises**. Par exemple, pour afficher les données sur les workflows ayant échoué, entrez `status=failed`.

Configurez l'extension Wavefront.

Utilisez l'extension Wavefront pour collecter des données de mesure sur votre système vRealize Orchestrator et vos workflows.

Conditions préalables

1 Vérifiez que Wavefront est activé dans le dispositif vRealize Orchestrator Appliance. Reportez-vous à Activation des extensions Opentracing et Wavefront.

2 Importez le certificat Wavefront :

   a Connectez-vous au centre de contrôle vRealize Orchestrator en tant qu'utilisateur **racine**.

   b Sélectionnez la page **Certificats**.

   c Cliquez sur le menu déroulant **Importer** et sélectionnez **Importer à partir de l'URL**.

   d Entrez l'URL de Wavefront et cliquez sur **Importer**.

3 Configurez un proxy Wavefront. Pour plus d'informations, reportez-vous au document Installation et gestion des proxies.

Procédure

1 Connectez-vous au centre de contrôle vRealize Orchestrator en tant qu'utilisateur **racine**.

2 Sélectionnez la page **Propriétés de l'extension**.

3 Sélectionnez l'extension Wavefront.

4 Configurez les propriétés de Wavefront.

Option	Description
Proxy	Adresse du proxy Wavefront.
Hôte	Facultatif. Adresse de l'hôte Wavefront.
Jeton	Facultatif. Le jeton d'API Wavefront. Pour plus d'informations sur la génération d'un jeton d'API Wavefront, reportez-vous à Génération d'un jeton d'API.
Préfixe	Ajoutez des étiquettes de préfixe pour chaque mesure envoyée à Wavefront. Les étiquettes de préfixe sont séparées par un symbole de point.

5 (Facultatif) Sélectionnez **Envoyer le tableau de bord par défaut au prochain démarrage**.

6 Cliquez sur **Enregistrer**.

Résultats

Vous avez configuré l'extension Wavefront pour vRealize Orchestrator.

Étape suivante

- Pour accéder aux mesures collectées par Wavefront, accédez au tableau de bord sur l'adresse entrée lors de la configuration.
- Pour obtenir des notifications sur des événements spécifiques dans votre environnement vRealize Orchestrator, vous pouvez utiliser des alertes Wavefront. Pour plus d'informations, reportez-vous à la documentation Alertes Wavefront.

Activer la synchronisation de l'heure pour vRealize Orchestrator

Vous pouvez activer la synchronisation de l'heure sur votre déploiement vRealize Orchestrator avec la ligne de commande vRealize Orchestrator Appliance.

Vous pouvez configurer la synchronisation de l'heure pour votre déploiement vRealize Orchestrator autonome ou en cluster à l'aide du protocole de communication NTP (Network Time Protocol). vRealize Orchestrator prend en charge deux configurations NTP mutuellement exclusives :

Configuration NTP	Description
ESXi	Cette configuration peut être utilisée lorsque le serveur ESXi hébergeant le dispositif vRealize Orchestrator Appliance est synchronisé avec un serveur NTP. Si vous utilisez un déploiement en cluster, tous les hôtes ESXi doivent être synchronisés avec un serveur NTP. Pour plus d'informations sur la configuration de NTP pour ESXi, reportez-vous à la section Configuration du protocole NTP (Network Time Protocol) sur un hôte ESXi à l'aide de vSphere Web Client. **Note** Si votre déploiement vRealize Orchestrator est migré vers un hôte ESXi qui n'est pas synchronisé avec un serveur NTP, vous pouvez rencontrer un décalage de l'horloge.
systemd	Cette configuration utilise le démon systemd-timesyncd pour synchroniser les horloges de votre déploiement vRealize Orchestrator. **Note** Par défaut, le démon systemd-timesyncd est activé, mais configuré sans serveur NTP. Si le dispositif vRealize Orchestrator Appliance utilise une configuration d'adresse IP dynamique, il peut utiliser n'importe quel serveur NTP reçu par le protocole DHCP.

Procédure

1. Connectez-vous à la ligne de commande du dispositif vRealize Orchestrator Appliance en tant qu'utilisateur **racine**.
2. Activez NTP avec ESXi.
   a. Exécutez la commande `vracli ntp esxi`.
   b. (Facultatif) Pour confirmer l'état de la configuration NTP, exécutez la commande `vracli ntp status`.
3. Activez NTP avec systemd.
   a. Exécutez la commande `vracli ntp systemd --set` *FQDN_or_IP_of_systemd_server*.

      Note Vous pouvez ajouter plusieurs serveurs NTP systemd en séparant leurs adresses réseau par une virgule. Chaque adresse réseau doit être placée entre guillemets simples. Par exemple, `vracli ntp systemd --set` *'ntp_address_1'*,*'ntp_address_2'*

   b. (Facultatif) Pour confirmer l'état de la configuration NTP, exécutez la commande `vracli ntp status`.

Résultats

Vous avez activé la synchronisation de l'heure pour votre déploiement vRealize Orchestrator.

Étape suivante

La configuration NTP peut échouer s'il existe une différence de temps de plus de 10 minutes entre le serveur NTP et le déploiement vRealize Orchestrator. Pour résoudre ce problème, redémarrez le dispositif vRealize Orchestrator Appliance.

Désactiver la synchronisation de l'heure pour vRealize Orchestrator

Vous pouvez désactiver la synchronisation de l'heure NTP (Network Time Protocol) sur votre déploiement vRealize Orchestrator en utilisant la ligne de commande du dispositif vRealize Orchestrator Appliance.

Vous pouvez également réinitialiser la configuration NTP de votre dispositif vRealize Orchestrator Appliance à l'état par défaut en exécutant la commande `vracli ntp reset`.

Conditions préalables

Vérifiez que vous avez configuré la synchronisation de l'heure avec ESXi ou systemd. Reportez-vous à Activer la synchronisation de l'heure pour vRealize Orchestrator.

Procédure

1. Connectez-vous à la ligne de commande du dispositif vRealize Orchestrator Appliance en tant qu'utilisateur **racine**.

2 Pour désactiver la synchronisation de l'heure avec ESXi ou systemd, exécutez la commande `vracli ntp disable`.

3 (Facultatif) Pour confirmer l'état de la configuration NTP, exécutez la commande `vracli ntp status`.

Configurer le CIDR Kubernetes de vRealize Orchestrator

Vous pouvez modifier les masques de sous-réseau du routage inter-domaines sans classe (Classless Inter-domain Routing, CIDR) après le déploiement.

Le dispositif vRealize Orchestrator Appliance configure un cluster Kubernetes et l'exécute. Les espaces et les services de ce cluster sont déployés dans des sous-réseau IPv4 distincts, représentés par le CIDR de cluster interne et le CIDR de service interne, respectivement. Les valeurs par défaut des masques de sous-réseau définies lors du déploiement OVF sont les suivantes :

Kubernetes network property	Default value	Property description
`cluster-cidr`	10.244.0.0/22	CIDR utilisé pour les espaces s'exécutant dans le cluster Kubernetes.
`service-cidr`	10.244.4.0/22	CIDR utilisé pour les services Kubernetes dans le cluster Kubernetes.

Les adresses réseau CIDR par défaut peuvent créer un conflit avec des réseaux privés externes que vous utiliserez peut-être. Dans de tels scénarios, vous pouvez modifier la configuration de ces valeurs CIDR pendant ou après le déploiement de votre dispositif vRealize Orchestrator Appliance.

Note Pour plus d'informations sur la modification de la configuration CIDR lors du déploiement du dispositif, reportez-vous à la section Télécharger et déployer le dispositif vRealize Orchestrator Appliance.

Conditions préalables

- Vérifiez que les valeurs d'adresses CIDR prennent en charge au moins 1 024 hôtes.
- Le CIDR de cluster interne et le CIDR de service interne ne doivent pas partager la même valeur de sous-réseau.
- La valeur CIDR de l'un des sous-réseaux ne peut pas inclure la valeur à ajouter à l'autre sous-réseau.

  Note Par exemple, la valeur `cluster-cidr` ne peut pas être **`10.244.4.0/22`** **`10.244.4.0/24`**, car cela inclurait la valeur de sous-réseau pour la propriété `service-cidr`. Chaque valeur de sous-réseau doit être ajoutée séparément.

Procédure

1 Connectez-vous au dispositif vRealize Orchestrator Appliance en tant qu'utilisateur **racine**.

2 Exécutez la commande `vracli upgrade exec -y --prepare --profile k8s-subnets`.

3 Sauvegardez votre déploiement vRealize Orchestrator en utilisant un snapshot de machine virtuelle (VM). Consultez la section Prendre un snapshot d'une machine virtuelle.

Attention vRealize Orchestrator 8.x ne prend actuellement pas en charge les snapshots de mémoire. Avant de prendre le snapshot de votre déploiement vRealize Orchestrator, vérifiez que l'option **Prendre un snapshot de la mémoire de la machine virtuelle** est désactivée.

4 Modifiez les valeurs des sous-réseaux de CIDR de cluster et de CIDR de service en exécutant la commande `vracli network k8s-subnets`.

```
vracli network k8s-subnets --cluster-cidr <CIDR_value> --service-cidr <CIDR_value>
```

5 Pour terminer le processus de configuration CIDR, exécutez la commande `vracli upgrade exec`.

Mettre à jour les paramètres DNS pour vRealize Orchestrator

Un administrateur peut mettre à jour les paramètres DNS du déploiement vRealize Orchestrator à l'aide de la commande `vracli network dns`.

Conditions préalables

Vérifiez que le service SSH du dispositif vRealize Orchestrator Appliance est activé. Reportez-vous à Activer ou désactiver l'accès SSH au dispositif vRealize Orchestrator Appliance.

Procédure

1 Connectez-vous à la ligne de commande de vRealize Orchestrator Appliance sur SSH en tant qu'utilisateur **racine**.

Note Pour les déploiements mis en cluster, connectez-vous au dispositif de n'importe quel nœud du cluster.

2 Pour définir de nouveaux serveurs DNS sur votre déploiement de vRealize Orchestrator, exécutez la commande `vracli network dns set`.

```
vracli network dns set --servers DNS1,DNS2
```

3 Vérifiez que les nouveaux serveurs DNS sont correctement appliqués à tous les nœuds vRealize Orchestrator en exécutant la commande `vracli network dns status`.

4 Pour arrêter les services vRealize Orchestrator dans votre déploiement, exécutez l'ensemble de commandes suivant :

```
/opt/scripts/svc-stop.sh
sleep 120
/opt/scripts/deploy.sh --onlyClean
```

5 Redémarrez les nœuds vRealize Orchestrator et attendez qu'ils démarrent complètement.

6 Connectez-vous à la ligne de commande pour chaque nœud vRealize Orchestrator via SSH et vérifiez que les nouveaux serveurs DNS sont répertoriés dans le fichier `/etc/resolve.conf`.

7 Pour démarrer les services vRealize Orchestrator, exécutez le script `/opt/scripts/deploy.sh` sur l'un des nœuds de votre déploiement.

Résultats

Les paramètres DNS vRealize Orchestrator sont modifiés comme indiqué.

Cas d'utilisation de la configuration et dépannage

8

Les cas d'utilisation de la configuration fournissent des flux de tâches que vous pouvez effectuer pour répondre à des exigences de configuration spécifiques de votre serveur vRealize Orchestrator et des rubriques de dépannage pour comprendre et résoudre un problème.

Ce chapitre contient les rubriques suivantes :

Vérifier le numéro de build du serveur vRealize Orchestrator

Dans certains scénarios, il peut être nécessaire de vérifier le numéro de build du serveur de votre déploiement vRealize Orchestrator.

Vous pouvez vérifier votre numéro de build du serveur vRealize Orchestrator en accédant à https://*your_orchestrator_FQDN*/vco/api/about. Le numéro de build de votre serveur s'affiche dans les balises `<ns2:build-number>`.

La vérification du numéro de build de votre serveur peut être utile dans des cas d'utilisation tels que la fourniture d'informations supplémentaires à une demande de support (SR) que vous avez enregistrée avec le support VMware.

Note Le numéro de build du serveur vRealize Orchestrator est différent de celui de votre vRealize Orchestrator Appliance. Pour vérifier le numéro de build de votre dispositif, connectez-vous à la ligne de commande vRealize Orchestrator Appliance et exécutez la commande `vracli version`. La vérification du numéro de build du dispositif peut vous aider à confirmer si votre mise à niveau vers la dernière version de vRealize Orchestrator est réussie.

Configurer le plug-in vRealize Orchestrator pour vSphere Web Client

Pour utiliser le plug-in vRealize Orchestrator pour vSphere Web Client, vous devez enregistrer vRealize Orchestrator en tant qu'extension de l'instance de vCenter Server.

Une fois que votre serveur vRealize Orchestrator est enregistré dans vCenter Single Sign-On et configuré pour fonctionner avec vCenter Server, vous devez enregistrer vRealize Orchestrator en tant qu'extension de vCenter Server.

Conditions préalables

- Vérifiez que l'accès SSH est activé pour le dispositif vRealize Orchestrator Appliance. Reportez-vous à Activer ou désactiver l'accès SSH au dispositif vRealize Orchestrator Appliance.
- Vous devez enregistrer vRealize Orchestrator dans l'authentification vSphere sur la même instance de Platform Services Controller sur laquelle s'authentifie votre instance de vCenter Server gérée.
- Copiez le fichier `vco-plugin.zip` dans le dispositif vRealize Orchestrator Appliance :
  a Téléchargez le fichier `vco-plugin.zip` à partir du Réseau Technologie VMware.
  b Ouvrez un client SSH.

  Note Pour les environnements Linux ou MacOS, vous pouvez utiliser l'interface de ligne de commande de terminal. Pour les environnements Windows, vous pouvez utiliser le client PuTTY.

  c Pour copier le fichier `vco-plugin.zip` , exécutez la commande secure copy.

```
For Linux/MacOS: scp ~/<zip_download_dir>/vco-plugin.zip
root@<orchestrator_FQDN_or_IP>:/data/vco/usr/lib/vco/downloads/vco-plugin.zip
```

```
For Windows: pscp C:\<zip_download_dir>\vco-plugin.zip root@<orchestrator_FQDN_or_IP>:/
data/vco/usr/lib/vco/downloads/vco-plugin.zip
```

Procédure

1. Connectez-vous à vRealize Orchestrator Client.
2. Accédez à **Bibliothèque > Workflows**.
3. Recherchez le workflow **Enregistrer vCenter Orchestrator en tant qu'extension de vCenter Server** et cliquez sur **Exécuter**.
4. Sélectionnez l'instance de vCenter Server dans laquelle vous souhaitez enregistrer vRealize Orchestrator.
5. Entrez https://*your_orchestrator_FQDN* ou l'URL de service de l'équilibrage de charge qui redirige les demandes vers les nœuds de serveur vRealize Orchestrator.

6 Cliquez sur **Exécuter**.

Annuler des workflows en cours d'exécution

Vous pouvez utiliser le centre de contrôle vRealize Orchestrator pour annuler des workflows qui ne se terminent pas correctement.

Procédure

1 Connectez-vous au centre de contrôle en tant qu'utilisateur **`racine`**.

2 Cliquez sur **Dépannage**.

3 Annulez des workflows en cours d'exécution.

Option	Description
Annuler toutes les exécutions de workflow	Entrez un ID de workflow pour annuler tous les jetons de ce workflow.
Annuler les exécutions de workflow par ID	Entrez tous les ID des jetons que vous voulez annuler. Séparez les ID avec une virgule.
Annulez tous les workflows en cours d'exécution.	Annulez tous les workflows en cours d'exécution sur le serveur.

Note Il se peut que les opérations d'annulation de workflows par ID échouent, car il n'existe aucune manière fiable d'annuler le thread d'exécution immédiatement.

Résultats

Lors du prochain démarrage du serveur, l'état des workflows est défini sur Annulé.

Activer le débogage du serveur vRealize Orchestrator

Vous pouvez démarrer le serveur vRealize Orchestrator en mode débogage pour déboguer les problèmes lors du développement d'un plug-in.

Conditions préalables

Installez et configurez l'outil de ligne de commande Kubernetes sur votre machine locale. Reportez-vous à Installer et configurer kubectl.

Procédure

1 Connectez-vous à la ligne de commande du dispositif vRealize Orchestrator Appliance en tant qu'utilisateur **racine**.

2 Exécutez la commande `kubectl -n prelude edit deployment vco-app`.

3 Modifiez le fichier de déploiement `YAML` en ajoutant une variable d'environnement de débogage au conteneur `vco-server-app`. La variable doit être ajoutée sous la section `env` du conteneur `vco-server-app`.

```
containers:
      - command:
      ...
        env:
        - name: DEBUG_PORT
          value: "your_desired_debug_port"
      ...
    name: vco-server-app
      ...
```

Note Lorsque vous ajoutez la variable d'environnement de débogage à la section `env`, vous devez suivre la mise en forme de la mise en retrait YAML comme présenté dans l'exemple précédent.

4 Enregistrez les modifications dans le fichier de déploiement.

Si la modification apportée au fichier de déploiement réussit, vous recevez le message `deployment.extensions/vco-app edited`.

5 Générez le fichier de configuration Kubernetes, en exécutant la commande `vracli dev kubeconfig`.

Comme kubeconfig est un environnement de développement, vous êtes invité à confirmer que vous souhaitez continuer. Entrez **`oui`** pour continuer ou **`non`** pour arrêter.

6 Copiez le contenu du fichier de configuration généré depuis `apiVersion: v1` jusqu'au contenu `client-key-data`.

7 Enregistrez le fichier de configuration Kubernetes généré sur votre machine locale.

8 Déconnectez-vous de vRealize Orchestrator Appliance.

9 Terminez la configuration du mode de débogage sur votre machine locale.

a Ouvrez un shell de ligne de commande.

b Liez la variable d'environnement *KUBECONFIG* au fichier de configuration enregistré.

Note Cet exemple est basé sur un environnement Linux.

```
export KUBECONFIG=/file/path/fileName
```

c Pour vérifier si les services sont en cours d'exécution, exécutez la commande `kubectl cluster-info`.

d Pour terminer la configuration du mode de débogage, exécutez la demande d'API Kubernetes suivante.

Note La valeur de la variable *localhost_debug_port* est le port défini dans la configuration de débogage distant de votre environnement de développement intégré. La valeur de la variable *vro_debug_port* est générée au cours de l'étape 3 de cette procédure.

```
kubectl port-forward pod/vco_app_pod_ID localhost_debug_port:vro_debug_port
```

Important Lors de la configuration de votre outil de débogage, fournissez les paramètres DNS et IP de la machine locale sur laquelle vous avez effectué la commande de transfert de port.

Résultats

Vous avez configuré le débogage du serveur pour votre dispositif vRealize Orchestrator Appliance.

Redimensionner les disques vRealize Orchestrator Appliance

Vous pouvez modifier la taille de disque du dispositif vRealize Orchestrator Appliance en modifiant les paramètres de taille de disque de la machine virtuelle vRealize Orchestrator Appliance dans vSphere.

Conditions préalables

Vérifiez que le service SSH du dispositif vRealize Orchestrator Appliance est activé. Reportez-vous à Activer ou désactiver l'accès SSH au dispositif vRealize Orchestrator Appliance.

Procédure

1 Vérifiez l'espace disque disponible actuellement dans le dispositif vRealize Orchestrator Appliance.

Note Les disques vRealize Orchestrator Appliance ont besoin d'au moins 20 pour cent d'espace disque libre.

a Connectez-vous à la ligne de commande de vRealize Orchestrator Appliance sur SSH en tant qu'utilisateur **racine**.

b Exécutez la commande `vracli disk-mgr`.

2 Redimensionnez le disque de la machine virtuelle vRealize Orchestrator Appliance dans vSphere.

   a Connectez-vous à vSphere Client en tant qu'**administrateur**.

   b Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Modifier les paramètres**.

   c Dans l'onglet **Matériel virtuel**, développez l'option **Disque dur** pour afficher et modifier les paramètres de disque, puis cliquez sur **OK**.

   Pour plus d'informations sur la modification de la taille de disque des machines virtuelles vSphere, reportez-vous à la section *Modifier la configuration de disque virtuel* dans *Administration d'une machine virtuelle vSphere*.

3 Déclenchez le redimensionnement automatique dans le système d'exploitation Photon OS.

   a Connectez-vous à la ligne de commande de vRealize Orchestrator Appliance sur SSH en tant qu'utilisateur **racine**.

   b Exécutez la commande `vracli disk-mgr resize`.

   Note Vous pouvez suivre la progression de la procédure de redimensionnement des disques dans `/var/log/vmware/prelude/disk_resize.log`.

   Vous avez redimensionné les disques vRealize Orchestrator Appliance.

4 Pour vérifier la réussite de la procédure de redimensionnement des disques, exécutez la commande `disk-mgr`.

```
vracli disk-mgr
```

Étape suivante

Pour résoudre les problèmes liés à la procédure de redimensionnement des disques, reportez-vous à l'article 79925 de la base de connaissances.

Dimensionnement de la mémoire du segment de mémoire du serveur vRealize Orchestrator

Vous pouvez dimensionner la taille du segment de mémoire du serveur vRealize Orchestrator en créant un profil personnalisé et en modifiant le fichier de mesures de ressources.

Vous pouvez ajuster la taille de la mémoire du segment de mémoire du serveur vRealize Orchestrator, de sorte que votre environnement d'orchestration puisse gérer des charges de travail variables. Par exemple, vous pouvez augmenter la mémoire du segment de mémoire de votre déploiement vRealize Orchestrator si vous prévoyez de gérer plusieurs instances de vCenter Server.

Conditions préalables

- Activez l'accès SSH au dispositif vRealize Orchestrator Appliance. Reportez-vous à Activer ou désactiver l'accès SSH au dispositif vRealize Orchestrator Appliance.
- Augmentez la RAM de la machine virtuelle sur laquelle vRealize Orchestrator est déployé jusqu'à l'incrément approprié suivant. Il est important qu'une quantité suffisante de mémoire soit disponible pour les services restants, c'est pourquoi les ressources vRealize Orchestrator Appliance doivent d'abord monter en puissance. Par exemple, si la mémoire de segment souhaitée est `7G`, la RAM vRealize Orchestrator Appliance doit être augmentée avec `4G` respectivement, car la soustraction entre la valeur de segment par défaut de `3G` et la mémoire de segment souhaitée est `4G`. Pour plus d'informations sur l'augmentation de la RAM d'une machine virtuelle dans vSphere, reportez-vous à la section *Modifier la configuration de la mémoire* dans *Administration d'une machine virtuelle vSphere*.

Procédure

1. Connectez-vous à la ligne de commande de vRealize Orchestrator Appliance sur SSH en tant qu'utilisateur **racine**.
2. Pour créer le répertoire de profils personnalisé et l'arborescence de répertoires requise utilisée lorsque le profil est actif, exécutez le script suivant :

```
vracli cluster exec -- bash -c 'base64 -d <<<
IyBDcmVhdGUgY3VzdG9tIHByb2ZpbGUgZGlyZWN0b3J5Cm1rZGlyIC1wIC9ldGMvdm13YXJlLXByZWx1ZGUvcHJvZml
sZXMvY3VzdG9tLXByb2ZpbGUvCgojIENyZWF0ZSB0aGUgcmVxdWlyZWQgZGlyZWN0b3J5IHRyZWUgdGhhdCB3aWxsIG
JlIHVzZWQgd2hlbiB0aGUgcHJvZmlsZSBpcyBhY3RpdmUKbWtkaXIgLXAgL2V0Yy92bXdhcmUtcHJlbHVkZS9wcm9ma
Wxlcy9jdXN0b20tcHJvZmlsZS9oZWxtL3ByZWx1ZGVfdmNvLwoKIyBDcmVhdGUgImNoZWNrIiBmaWxlIHRoYXQgaXMg
YW4gZXhlY3V0YWJsZSBmaWxlIHJ1biBieSBkZXBsb3kgc2NyaXB0LgpjYXQgPDxFT0YgPiAvZXRjL3Ztd2FyZS1wcmV
sdWRlL3Byb2ZpbGVzL2N1c3RvbS1wcm9maWxlL2NoZWNrCiMhL2Jpbi9iYXNoCmV4aXQgMApFT0YKY2htb2QgNzU1IC
9ldGMvdm13YXJlLXByZWx1ZGUvcHJvZmlsZXMvY3VzdG9tLXByb2ZpbGUvY2hlY2sKCiMgQ29weSB2Uk8gcmVzb3VyY
2UgbWV0cmljcyBmaWxlIHRvIHlvdXIgY3VzdG9tIHByb2ZpbGUKY2F0IDw8RU9GID4gL2V0Yy92bXdhcmUtcHJlbHVk
ZS9wcm9maWxlcy9jdXN0b20tcHJvZmlsZS9oZWxtL3ByZWx1ZGVfdmNvLzkwLXJlc291cmNlcy55YW1sCnBvbHlnbG9
0UnVubmVyTWVtb3J5TGltaXQ6IDYwMDBNCnBvbHlnbG90UnVubmVyTWVtb3J5UmVxdWVzdDogMTAwME0KcG9seWdsb3
RSdW5uZXJNZW1vcnlMaW1pdFZjbzogNTYwME0KCnNlcnZlck1lbW9yeUxpbWl0OiA2RwpzZXJ2ZXJNZW1vcnlSZXF1Z
XN0OiA1RwpzZXJ2ZXJKdm1IZWFwTWF4OiA0RwoKY29udHJvbENlbnRlck1lbW9yeUxpbWl0OiAxLjVHCmNvbnRyb2xD
ZW50ZXJNZW1vcnlSZXF1ZXN0OiA3MDBtCkVPRgpjaG1vZCA2NDQgL2V0Yy92bXdhcmUtcHJlbHVkZS9wcm9maWxlcy9
jdXN0b20tcHJvZmlsZS9oZWxtL3ByZWx1ZGVfdmNvLzkwLXJlc291cmNlcy55YW1sCg== | bash'
```

3. Modifiez le fichier de mesures de ressources dans votre profil personnalisé avec les valeurs de mémoire souhaitées.

```
vi /etc/vmware-prelude/profiles/custom-profile/helm/prelude_vco/90-resources.yaml
```

4. Enregistrez les modifications dans le fichier de mesures de ressources et exécutez le script `deploy.sh`.

```
/opt/scripts/deploy.sh
```

Résultats

Vous avez modifié la taille de la mémoire du segment de mémoire de votre serveur vRealize Orchestrator.

Récupération d'urgence de vRealize Orchestrator à l'aide de Site Recovery Manager

Vous devez configurer Site Recovery Manager pour protéger votre vRealize Orchestrator. Sécurisez cette protection en terminant les tâches de configuration courantes pour Site Recovery Manager.

Préparer l'environnement

Vous devez vous assurer que vous répondez aux conditions préalables suivantes avant de commencer la configuration de Site Recovery Manager.

- Vérifiez que vSphere 6.0 ou version ultérieure est installé sur les sites protégés et de récupération.
- Vérifiez que vous utilisez Site Recovery Manager 8.1 ou une version ultérieure.
- Vérifiez que vRealize Orchestrator est configuré.

Configurer des machines virtuelles pour vSphere Replication

Vous devez configurer les machines virtuelles pour la réplication vSphere Replication ou basée sur la baie en vue d'utiliser Site Recovery Manager.

Pour activer vSphere Replication sur les machines virtuelles requises, procédez comme suit.

Procédure

1. Dans vSphere Web Client, sélectionnez une machine virtuelle sur laquelle vSphere Replication doit être activé, puis cliquez sur **Actions > Toutes les actions de réplication vSphere > Configurer la réplication**.
2. Dans la fenêtre **Type de réplication**, sélectionnez **Répliquer vers un vCenter Server** et cliquez sur **Suivant**.
3. Dans la fenêtre **Site cible**, sélectionnez le vCenter du site de récupération et cliquez sur **Suivant**.
4. Dans la fenêtre **Serveur de réplication**, sélectionnez un serveur vSphere Replication et cliquez sur **Suivant**.
5. Dans la fenêtre **Emplacement cible**, cliquez sur **Modifier** et sélectionnez la banque de données cible, où les fichiers répliqués seront stockés, puis cliquez sur **Suivant**.
6. Dans la fenêtre **Options de réplication**, conservez les paramètres par défaut et cliquez sur **Suivant**.

7 Dans la fenêtre **Paramètres de récupération**, indiquez l'heure pour l'**Objectif de point de récupération (RPO)** et les **Instances ponctuelles**, et cliquez sur **Suivant**.

8 Dans la fenêtre **Prêt à terminer**, vérifiez les paramètres et cliquez sur **Terminer**.

9 Répétez ces étapes pour toutes les machines virtuelles sur lesquelles vSphere Replication doit être activé.

Créer des groupes de protection

Vous pouvez créer des groupes de protection pour permettre à Site Recovery Manager de protéger vos machines virtuelles.

Vous pouvez organiser les groupes de protection en dossiers. L'onglet **Groupes de protection** affiche les noms des groupes de protection, mais n'affiche pas le dossier dans lequel ils sont placés. Si vous avez deux groupes de protection portant le même nom dans des dossiers différents, il peut être difficile de les différencier. Par conséquent, veillez à ce que chaque nom de groupe de protection soit unique dans tous les dossiers. Dans des environnements dans lesquels tous les utilisateurs n'ont pas de privilèges de vue pour tous les dossiers, pour être sûr de l'unicité des noms des groupes de protection, ne placez pas de groupes de protection dans des dossiers.

Lorsque vous créez des groupes de protection, patientez afin de vous assurer que les opérations se terminent comme prévu. Assurez-vous que Site Recovery Manager crée le groupe de protection et que la protection des machines virtuelles du groupe est effective.

Conditions préalables

Vérifiez que vous avez effectué l'une des tâches suivantes :

- Inclure des machines virtuelles dans les banques de données pour lesquelles vous avez configuré une réplication basée sur la baie.
- Respecter les conditions requises dans les *Conditions préalables pour les groupes de protection par stratégie de stockage* et examiner les *Limitations des groupes de protection par stratégie de stockage* dans le guide *Administration de Site Recovery Manager*.
- vSphere Replication configuré sur vos machines virtuelles
- Effectuez une partie ou l'intégralité des actions ci-dessus.

Procédure

1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.

2 Dans l'onglet Accueil de Site Recovery, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.

3 Sélectionnez l'onglet **Groupes de protection**, puis cliquez sur **Nouveau** pour créer un groupe de protection.

4 Dans la page Nom et description, entrez un nom et une description pour le groupe de protection, sélectionnez une direction, puis cliquez sur **Suivant**.

5 Sur la page Type de groupe de protection, sélectionnez le groupe de protection et cliquez sur **Suivant**.

Option	Action
Créer un groupe de protection pour la réplication basée sur la baie	Sélectionnez **Groupes de banque de données (réplication basée sur la baie)** et sélectionnez une paire de baies.
Créer un groupe de protection vSphere Replication	Sélectionnez **Machines virtuelles individuelles (vSphere Replication)**.
Créer un groupe de protection par stratégie de stockage	Sélectionnez **Stratégies de stockage (réplication basée sur la baie)**.

6 Sélectionnez des groupes de banque de données, des machines virtuelles ou des stratégies de stockage à ajouter au groupe de protection.

Option	Action
Groupes de protection pour la réplication basée sur les baies	Sélectionnez les groupes de banque de données et cliquez sur **Suivant**. Lorsque vous sélectionnez un groupe de banques de données, les machines virtuelles que le groupe contient apparaissent dans le tableau Machines virtuelles.
Groupes de protection vSphere Replication	Sélectionnez des machines virtuelles dans la liste, puis cliquez sur **Suivant**. Seules les machines virtuelles configurées pour vSphere Replication et ne se trouvant pas encore dans un groupe de protection apparaissent dans la liste.
Groupes de protection par stratégie de stockage	Sélectionnez les stratégies de stockage dans la liste, puis cliquez sur **Suivant**.

7 Sur la page Plan de récupération, vous pouvez éventuellement ajouter le groupe de protection à un plan de récupération.

Option	Action
Ajouter à un plan de récupération existant	Ajoute le groupe de protection à un plan de récupération existant.
Ajouter à un nouveau plan de récupération	Ajoute le groupe de protection à un nouveau plan de récupération. Si vous sélectionnez cette option, vous devez entrer un nom pour le plan de récupération.
Ne pas ajouter à un plan de récupération maintenant.	Sélectionnez cette option si vous ne souhaitez pas ajouter le groupe de protection à un plan de récupération.

8 Passez en revue vos paramètres et cliquez sur **Terminer**.

Vous pouvez suivre la progression de la création du groupe de protection dans l'onglet **Groupe de protection**.

- Pour la réplication basée sur la baie et les groupes de protection vSphere Replication, si Site Recovery Manager a correctement appliqué les mappages d'inventaire aux machines virtuelles protégées, l'état de protection du groupe de protection est *OK*.

- Pour les groupes de protection par stratégie de stockage, si Site Recovery Manager a correctement protégé toutes les machines virtuelles associées à la stratégie de stockage, l'état de protection du groupe de protection est *OK*.
- Pour la réplication basée sur la baie et les groupes de protection vSphere Replication, si vous n'avez pas configuré les mappages d'inventaire ou si Site Recovery Manager n'a pas pu les appliquer, l'état de protection du groupe de protection est *Non configuré*.
- Pour les groupes de protection par stratégie de stockage, si Site Recovery Manager ne peut pas protéger toutes les machines virtuelles associées à la stratégie de stockage, l'état de protection du groupe de protection est *Non configuré*.

Étape suivante

Pour la réplication basée sur la baie et les groupes de protection vSphere Replication, si l'état de protection des groupes de protection est *Non configuré*, appliquez des mappages d'inventaire aux machines virtuelles :

- Pour appliquer des mappages d'inventaire à l'échelle du site ou pour vérifier que les mappages d'inventaire que vous avez déjà définis sont valides, reportez-vous à la section *Configurer les mappages d'inventaire* dans le guide *Administration de Site Recovery Manager*. Pour appliquer ces mappages à toutes les machines virtuelles, reportez-vous à *Appliquer des mappages d'inventaire à tous les membres d'un groupe de protection* dans le guide *Administration de Site Recovery Manager*.
- Pour appliquer individuellement des mappages d'inventaire à chaque machine virtuelle du groupe de protection, reportez-vous à la section *Configurer des mappages d'inventaire pour une machine virtuelle individuelle dans un groupe de protection* dans le guide *Administration de Site Recovery Manager*.

Pour les groupes de protection par stratégie de stockage, si l'état de protection du groupe de protection est *Non configuré*, vérifiez que vous avez respecté les conditions requises dans *Conditions préalables pour les groupes de protection par stratégie de stockage* et examiné les *Limitations des groupes de protection par stratégie de stockage* dans le guide *Administration de Site Recovery Manager*.

Créer un plan de récupération

Vous pouvez créer un plan de récupération pour établir la manière dont les machines virtuelles seront récupérées par Site Recovery Manager.

Procédure

1. Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
2. Dans l'onglet Accueil de Site Recovery, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
3. Sélectionnez l'onglet **Plans de récupération**, puis cliquez sur **Nouveau** pour créer un plan de récupération.

4 Entrez un nom, une description et une direction pour le plan, sélectionnez un dossier, puis cliquez sur **Suivant**.

5 Sélectionnez le type du groupe dans le menu.

Option	Description
Groupes de protection pour des machines virtuelles individuelles ou des groupes de banque de données	Sélectionnez cette option pour créer un plan de récupération contenant une réplication basée sur la baie et des groupes de protection vSphere Replication.
Groupes de protection par stratégie de stockage	Sélectionnez cette option pour créer un plan de récupération contenant des groupes de protection par stratégie de stockage. Si vous utilisez un stockage étendu, sélectionnez cette option.

6 Sélectionnez un ou plusieurs groupes de protection à récupérer, et cliquez sur **Suivant**.

7 Dans le menu déroulant **Réseau de test**, sélectionnez un réseau à utiliser lors du test de récupération et cliquez sur **Suivant**.

S'il n'existe aucun mappage au niveau du site, l'option par défaut **Utiliser le mappage au niveau du site** crée un réseau de test isolé.

8 Consultez les informations récapitulatives et cliquez sur **Terminer** pour créer le plan de récupération.

Organiser les plans de récupération dans des dossiers

Pour contrôler l'accès de différents utilisateurs ou groupes à des plans de récupération, vous pouvez organiser vos plans de récupération dans des dossiers.

L'organisation de plans de récupération en dossiers est utile si vous disposez de nombreux plans de récupération. Vous pouvez limiter l'accès aux plans de récupération en les plaçant dans des dossiers et en attribuant différentes autorisations aux dossiers pour différents utilisateurs ou groupes. Pour plus d'informations sur l'attribution d'autorisations aux dossiers, reportez-vous à *Attribuer des rôles et des autorisations Site Recovery Manager* dans le guide *Administration de Site Recovery Manager*.

Procédure

1 Dans l'onglet Accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.

2 Cliquez sur l'onglet **Plans de récupération** et, dans le volet de gauche, cliquez avec le bouton droit sur **Plans de récupération** et cliquez sur **Nouveau dossier**.

3 Entrez un nom pour le dossier à créer, puis cliquez sur **Ajouter**.

4 Ajoutez des plans de récupération nouveaux ou existants au dossier.

Option	Description
Créer un nouveau plan de récupération	Cliquez avec le bouton droit sur le dossier, puis sélectionnez **Nouveau plan de récupération**.
Ajouter un plan de récupération existant	Cliquez avec le bouton droit sur un plan de récupération dans l'arborescence d'inventaire et cliquez sur **Déplacer**. Sélectionnez un dossier cible et cliquez sur **Déplacer**.

Modifier un plan de récupération

Vous pouvez modifier un plan de récupération, afin de changer les propriétés que vous avez spécifiées lors de sa création. Vous pouvez modifier les plans de récupération à partir du site protégé ou du site de récupération.

Procédure

1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.

2 Dans l'onglet Accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.

3 Cliquez sur l'onglet **Plans de récupération**, cliquez avec le bouton droit sur un plan de récupération et cliquez sur **Modifier**.

4 (Facultatif) Modifiez le nom ou la description du plan et cliquez sur **Suivant**.

Vous ne pouvez pas modifier la direction et l'emplacement du plan de récupération.

5 (Facultatif) Sélectionnez ou désélectionnez un ou plusieurs groupes de protection pour les ajouter ou les retirer du plan, puis cliquez sur **Suivant**.

6 (Facultatif) Dans le menu déroulant, sélectionnez un réseau de test différent sur le site de récupération, puis cliquez sur **Suivant**.

7 Consultez les informations récapitulatives et cliquez sur **Terminer** pour appliquer les modifications spécifiées au plan de récupération.

Vous pouvez suivre la mise à jour du plan dans la vue **Tâches récentes**.

Configuration des propriétés du système

9

Vous pouvez définir les propriétés du système pour modifier le comportement par défaut d'Orchestrator.

Ce chapitre contient les rubriques suivantes :

Configuration de l'accès au système de fichiers du serveur pour les workflows et les actions

Dans vRealize Orchestrator, les workflows et les actions ont un accès limité à des répertoires de système de fichiers spécifiques. Vous pouvez étendre l'accès à d'autres parties du système de fichiers du serveur en modifiant le fichier de configuration `js-io-rights.conf`.

Règles dans le fichier js-io-rights.conf autorisant l'accès en écriture au système vRealize Orchestrator

Le fichier `js-io-rights.conf` contient des règles qui autorisent l'accès en écriture à des répertoires définis dans le système de fichiers du serveur.

Contenu obligatoire du fichier js-io-rights.conf

Chaque ligne du fichier `js-io-rights.conf` doit être au format suivant :

- Un signe plus (`+`) ou moins (`-`) pour indiquer si les droits sont autorisés ou refusés
- Les niveaux de droits lire (`r`), écrire (`w`) et exécuter (`x`)

- Chemin d'accès auquel appliquer les droits.

  Note Le dossier racine du fichier `js-io-rights.conf` est toujours `/var/run/vco`. Dans le système de fichiers vRealize Orchestrator Appliance, ce dossier se trouve sous `/data/vco/var/run/vco`. Tout le contenu ayant accès au système de fichiers vRealize Orchestrator doit être mappé sous ce dossier racine.

Contenu par défaut du fichier js-io-rights.conf

Le contenu par défaut du fichier de configuration de `js-io-rights.conf` dans Orchestrator Appliance est le suivant :

```
-rwx /
+rwx /var/run/vco
+rx /etc/vco
-rwx /etc/vco/app-server/security/
+rx /var/log/vco/
```

Les deux premières lignes du fichier de configuration `js-io-rights.conf` par défaut autorisent les droits d'accès suivants :

`-rwx /`

Tout accès au système de fichiers est refusé.

`+rwx /var/run/vco`

L'accès en lecture, écriture et exécution est autorisé dans le répertoire `/var/run/vco`.

Règles dans le fichier js-io-rights.conf

vRealize Orchestrator résout les droits d'accès dans l'ordre dans lequel ils figurent dans le fichier `js-io-rights.conf`. Chaque ligne peut remplacer les lignes précédentes.

Important Vous pouvez autoriser l'accès à toutes les parties du système de fichiers en définissant `+rwx /` dans le fichier `js-io-rights.conf`. Toutefois, cela représente un risque de sécurité élevé.

Configurer l'accès au système de fichiers du serveur pour les workflows et les actions

Pour modifier les parties du système de fichiers du serveur auxquelles les workflows et l'API de vRealize Orchestrator ont accès, modifiez le fichier de configuration `js-io-rights.conf`. Le fichier `js-io-rights.conf` est créé lorsqu'un workflow tente d'accéder au système de fichiers du serveur vRealize Orchestrator.

Procédure

1 Connectez-vous à la ligne de commande du dispositif vRealize Orchestrator Appliance en tant qu'utilisateur **racine**.

2 Accédez au répertoire `/data/vco/var/run/vco/`

3 Ouvrez le fichier de configuration `js-io-rights.conf` dans un éditeur de texte.

4 Ajoutez les lignes nécessaires au fichier `js-io-rights.conf` pour autoriser ou refuser l'accès aux zones du système de fichiers.

   Par exemple, la ligne suivante refuse les droits d'exécution dans le répertoire `/data/vco/var/run/vco/noexec` :

   ```
   -x /data/vco/var/run/vco/noexec
   ```

   `/data/vco/var/run/vco/noexec` conserve les droits d'exécution, mais `/data/vco/var/run/vco/noexec/bar` ne les conserve pas. Les deux répertoires restent lisibles et inscriptibles.

Résultats

Vous avez modifié les droits d'accès au système de fichiers pour les workflows et pour l'API de vRealize Orchestrator.

Définir l'accès aux commandes du système d'exploitation pour les workflows et les actions

vRealize Orchestrator API propose une catégorie de scripts, `Command`, qui exécute les commandes dans le système d'exploitation hôte du serveur vRealize Orchestrator. Pour éviter tout accès non autorisé à l'hôte du serveur Orchestrator, les applications vRealize Orchestrator ne disposent, par défaut, d'aucune autorisation pour exécuter la catégorie `Command`. Si les applications vRealize Orchestrator nécessitent une autorisation pour exécuter des commandes sur le système d'exploitation hôte, vous pouvez activer la classe de script `Command`.

Vous autorisez l'utilisation de la catégorie `Command` en définissant une propriété système de configuration de vRealize Orchestrator.

Procédure

1 Connectez-vous au centre de contrôle en tant qu'utilisateur **`racine`**.

2 Cliquez sur **Propriétés du système**.

3 Cliquez sur **Nouveau**.

4 Dans la zone de texte **Clé**, entrez **`com.vmware.js.allow-local-process`**.

5 Dans la zone de texte **Valeur**, entrez **`true`**.

6 Dans la zone de texte **Description**, entrez une description de la propriété système.

7 Cliquez sur **Ajouter**.

8 Cliquez sur **Enregistrer les modifications** à partir du menu contextuel.

   Un message indique que vos modifications sont correctement enregistrées.

9 Attendez que le serveur vRealize Orchestrator redémarre.

Résultats

Vous avez accordé des autorisations aux applications vRealize Orchestrator pour exécuter des commandes locales dans le système d'exploitation hôte du serveur vRealize Orchestrator.

Note En définissant la propriété système `com.vmware.js.allow-local-process` sur `true`, vous autorisez la catégorie de script `Command` à écrire à n'importe quel emplacement dans le système de fichiers. Cette propriété remplace toutes les autorisations d'accès au système de fichiers que vous avez définies dans le fichier `js-io-rights.conf` pour la catégorie de script `Command` uniquement. Les autorisations d'accès au système de fichiers que vous définissez dans le fichier `js-io-rights.conf` s'appliquent toujours à toutes les catégories de script autres que `Command`.

Définir l'accès du JavaScript aux classes Java

Par défaut, vRealize Orchestrator limite l'accès JavaScript à un ensemble limité de catégories Java. Si vous demandez un accès JavaScript à un éventail plus large de catégories Java, vous devez définir une propriété système vRealize Orchestrator.

Accorder au moteur JavaScript le plein accès à la machine virtuelle Java (ou JVM) représente des enjeux de sécurité potentiels. Des scripts malformés ou malveillants peuvent alors avoir accès à l'ensemble des composants système auxquels l'utilisateur exécutant le serveur vRealize Orchestrator a accès. Par conséquent, le moteur JavaScript de vRealize Orchestrator ne peut accéder par défaut qu'aux classes présentes dans le module `java.util.*`.

Si un accès JavaScript à des classes en dehors du module `java.util.*` est requis, vous avez la possibilité de dresser la liste des modules Java pour lesquels vous accordez l'accès au JavaScript dans un fichier de configuration. Ne vous reste plus qu'à définir la propriété système `com.vmware.scripting.rhino-class-shutter-file` pour qu'elle pointe sur ledit fichier.

Procédure

1 Créez un fichier texte de configuration pour y conserver la liste des modules Java pour lesquels vous accordez un accès au JavaScript.

   Par exemple, pour accorder l'accès du JavaScript à la totalité des classes se trouvant dans le module `java.net`, ainsi qu'à la classe `java.lang.Object`, il suffit d'ajouter le contenu suivant au fichier.

   ```
   java.net.*
   java.lang.Object
   ```

2 Entrez un nom pour le fichier de configuration.

3 Enregistrez le fichier de configuration dans le sous-répertoire `/data/vco/usr/lib/vco`.

   Note Le fichier de configuration ne peut pas être enregistré dans un autre répertoire.

4 Connectez-vous au centre de contrôle en tant qu'utilisateur **racine**.

5 Cliquez sur **Propriétés du système**.

6 Cliquez sur **Nouveau**.

7 Dans la zone de texte **Clé**, saisissez **com.vmware.scripting.rhino-class-shutter-file**.

8 Dans la zone de texte **Valeur**, entrez `vco/usr/lib/vco/your_configuration_file_subdirectory`.

9 Dans la zone de texte **Description**, entrez une description de la propriété système.

10 Cliquez sur **Ajouter**.

11 Cliquez sur **Enregistrer les modifications** à partir du menu contextuel.

Un message indique que vos modifications sont correctement enregistrées.

12 Attendez que le serveur vRealize Orchestrator redémarre.

Résultats

Le moteur JavaScript a désormais accès aux classes Java que vous avez indiquées.

Définir la propriété de délai d'expiration personnalisé

Lorsque vCenter Server est surchargé, il faut plus de temps pour renvoyer la réponse au serveur vRealize Orchestrator que les 20 000 millisecondes définies par défaut. Pour éviter cette situation, vous devez modifier le fichier de configuration de vRealize Orchestrator pour augmenter le délai d'expiration par défaut.

Si le délai par défaut expire avant l'achèvement de certaines opérations, le journal du serveur vRealize Orchestrator contient des erreurs.

```
Operation 'getPropertyContent' total time : '5742228' for 1823 calls, mean time : '3149.0', min time : '0', max time : '32313' Timeout, unable to get property 'info' com.vmware.vmo.plugin.vi4.model.TimeoutException
```

Procédure

1 Connectez-vous au centre de contrôle en tant qu'utilisateur **racine**.

2 Cliquez sur **Propriétés du système**.

3 Cliquez sur **Nouveau**.

4 Dans la zone de texte **Clé**, tapez **com.vmware.vmo.plugin.vi4.waitUpdatesTimeout**.

5 Dans la zone de texte **Valeur**, entrez le nouveau délai d'expiration en millisecondes.

6 (Facultatif) Dans la zone de texte **Description**, saisissez une description pour la propriété système.

7 Cliquez sur **Ajouter**.

8 Cliquez sur **Enregistrer les modifications** à partir du menu contextuel.

Un message indique que vos modifications sont correctement enregistrées.

9 Redémarrez le serveur Orchestrator.

Résultats

La valeur que vous indiquez remplace le paramètre de délai d'expiration par défaut fixé à 20 000 secondes.

Ajout d'un connecteur JDBC pour le plug-in SQL vRealize Orchestrator

Cet exemple montre comment vous pouvez ajouter un connecteur MySQL pour le plug-in SQL vRealize Orchestrator.

Procédure

1 Ajoutez le fichier. jar du connecteur MySQL au dispositif vRealize Orchestrator Appliance.

a Connectez-vous à la ligne de commande de vRealize Orchestrator Appliance sur SSH en tant qu'utilisateur **racine**.

b Accédez au répertoire `/data/vco/var/run/vco`.

```
cd /data/vco/var/run/vco
```

c Créez un répertoire `plugins/SQL/lib/`.

```
mkdir -p plugins/SQL/lib/
```

d Copiez votre fichier MySQL connector.jar de votre machine locale vers le répertoire `/data/vco/var/run/vco/plugins/SQL/lib/` en exécutant une commande Secure Copy (SCP).

```
scp ~/local_machine_dir/your_mysql_connector.jar root@orchestrator_FQDN_or_IP:/
data/vco/var/run/vco/plugins/SQL/lib/
```

Note Vous pouvez également utiliser d'autres méthodes pour copier votre fichier connector.jar sur le dispositif vRealize Orchestrator Appliance, tel que PSCP.

2 Ajoutez la nouvelle propriété MySQL au centre de contrôle.

a Connectez-vous au centre de contrôle en tant qu'utilisateur **racine**.

b Sélectionnez **Propriétés du système**.

c Cliquez sur **Nouveau**.

d Sous la **Clé**, entrez **`o11n.plugin.SQL.classpath`**.

e Sous la **Valeur**, entrez **`/var/run/vco/plugins/SQL/lib/your_mysql_connector.jar`**.

Note La zone de texte valeur peut inclure plusieurs connecteurs JDBC. Chaque connecteur JDBC est séparé par un point-virgule (« ; »). Par exemple :

```
/var/run/vco/plugins/SQL/lib/your_mysql_connector.jar;/var/run/vco/plugins/SQL/lib/
your_mssql_connector.jar;/var/run/vco/plugins/SQL/lib/your_other_connector.jar
```

f (Facultatif) Entrez une description pour la propriété du système MySQL.

g Cliquez sur **Ajouter** et attendez que le serveur vRealize Orchestrator redémarre.

Note N'enregistrez pas le fichier connector.jar JDBC dans un autre répertoire et ne définissez pas une valeur différente pour la propriété `o11n.plugin.SQL.classpath`, car cela rend le connecteur JDBC indisponible pour votre déploiement vRealize Orchestrator.

Définir la tâche planifiée et la propriété de renouvellement du jeton d'authentification de stratégie

Gérez la manière dont vous pouvez activer le renouvellement des jetons d'authentification utilisés dans les tâches ou les stratégies planifiées en définissant une propriété système.

Une tâche planifiée est configurée par des utilisateurs non-administrateurs dans vRealize Orchestrator Client sans heure de fin. Le jeton d'authentification de ce workflow planifié expire huit heures après l'heure de début spécifiée. Outre les tâches planifiées, ce jeton d'authentification est également utilisé pour des stratégies vRealize Orchestrator. Pour vous assurer que les workflows ou les stratégies planifiés dans le déploiement vRealize Orchestrator continuent à s'exécuter, vous pouvez définir une propriété système dans le centre de contrôle.

Note Les jetons d'authentification ne peuvent pas être renouvelés après 90 jours de leur date de début initiale.

Conditions préalables

Vérifiez que votre déploiement vRealize Orchestrator utilise un fournisseur d'authentification vRealize Automation ou qu'il est intégré dans vRealize Automation. La propriété système `com.vmware.o11n.auth.csp.renewTokens` n'est pas disponible pour les déploiements vRealize Orchestrator authentifiés avec vSphere.

Procédure

1 Connectez-vous au centre de contrôle en tant qu'utilisateur **racine**.

2 Sélectionnez **Propriétés du système**.

3 Cliquez sur **Nouveau**.

4 Sous **Clé**, entrez **`com.vmware.o11n.auth.csp.renewTokens`**.

5 Sous **Valeur**, entrez **`true`**.

Note Pour les déploiements de vRealize Orchestrator dans vRealize Automation et dans vRealize Automation Cloud, les workflows au long cours démarrés à partir de vRealize Automation endommagent le jeton d'authentification après son expiration. Le jeton est défini pour expirer huit heures après l'heure de début spécifiée.

6 (Facultatif) Entrez une description pour la nouvelle propriété système.

7 Cliquez sur **Ajouter** et attendez que le serveur vRealize Orchestrator redémarre.

Pour aller plus loin

10

Lorsque vous avez installé et configuré vRealize Orchestrator, vous pouvez utiliser vRealize Orchestrator pour automatiser les processus fréquemment répétés liés à la gestion de l'environnement virtuel.

- Connectez-vous à vRealize Orchestrator Client, exécutez et planifiez des workflows sur les objets d'inventaire vCenter Server ou d'autres objets auxquels vRealize Orchestrator a accès via ses plug-ins. Voir *Utilisation de VMware vRealize Orchestrator Client*.
- Dupliquez et modifiez les workflows standard de vRealize Orchestrator et écrivez vos propres actions et workflows pour automatiser les opérations dans vCenter Server.
- Pour étendre la fonctionnalité de la plate-forme vRealize Orchestrator, développez des plug-ins.
- Gérez votre inventaire vRealize Orchestrator dans plusieurs instances de vRealize Orchestrator avec l'intégration d'un référentiel Git distant. Reportez-vous à *Utilisation de VMware vRealize Orchestrator Client*.
- Exécutez les workflows sur vos objets d'inventaire vSphere à l'aide de vSphere Web Client.