

Installation et configuration de VMware vRealize Orchestrator

vRealize Orchestrator 7.5

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

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

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

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

Copyright © 2008-2018 VMware, Inc. Tous droits réservés. [Informations relatives aux copyrights et marques commerciales.](#)

Table des matières

Installation et configuration de VMware vRealize Orchestrator	6
1 Introduction à VMware vRealize Orchestrator	7
Fonctionnalités clés de la plate-forme Orchestrator	7
Types d'utilisateurs d'Orchestrator et responsabilités associées	10
Architecture d'Orchestrator	11
Plug-ins Orchestrator	11
2 Configuration requise du système pour Orchestrator	13
Configuration matérielle requise pour le dispositif Orchestrator Appliance	13
Navigateurs pris en charge par Orchestrator	14
Configuration requise pour la base de données d'Orchestrator	14
Logiciel inclus dans le dispositif Orchestrator Appliance	14
Niveau de prise en charge de l'internationalisation	14
Ports réseau d'Orchestrator	15
3 Installation des composants vRealize Orchestrator	17
Configuration de vCenter Server	17
Méthodes d'authentification	18
4 Installation de vRealize Orchestrator	19
Télécharger et déployer le dispositif vRealize Orchestrator Appliance	19
Mettre sous tension le dispositif vRealize Orchestrator et ouvrir la page d'accueil	21
Modifier le mot de passe racine	21
Activer ou désactiver la connexion administrateur SSH sur le dispositif vRealize Orchestrator Appliance	22
Configurer les paramètres réseau du dispositif vRealize Orchestrator Appliance	22
5 Configuration initiale	24
Configuration d'un serveur Orchestrator autonome	24
Configurer un serveur Orchestrator autonome avec l'authentification vRealize Automation	24
Configurer un serveur Orchestrator autonome avec l'authentification vSphere	26
Ports réseau d'Orchestrator	28
Connexion à la base de données Orchestrator	29
Gérer les certificats	29
Gérer les certificats Orchestrator	29
Configurer les plug-ins Orchestrator	32

Gérer les plug-Ins vRealize Orchestrator	32
Installer ou mettre à jour un plug-in vRealize Orchestrator	33
Désinstaller un plug-in	33
Disponibilité et évolutivité d'Orchestrator	34
Configurer un cluster d'instances de vRealize Orchestrator dans l'interface VAMI	35
Surveiller un cluster Orchestrator	36
Activer le mode synchrone pour le cluster Orchestrator	37
Promouvoir un nœud de réplica Orchestrator à l'état de nœud principal	38
Supprimer un nœud de cluster Orchestrator	38
Configuration du programme d'amélioration du produit	39
Catégories d'informations envoyées à VMware	39
Rejoindre le programme d'amélioration du produit	39
6 Utilisation des services d'API	40
Gestion des certificats SSL via l'API REST	40
Supprimer un certificat SSL à l'aide de l'API REST	41
Importer des certificats SSL à l'aide de l'API REST	41
Créer un keystore à l'aide de l'API REST	43
Supprimer un keystore à l'aide de l'API REST	43
Ajouter une clé à l'aide de l'API REST	44
Automatisation de la configuration d'Orchestrator à l'aide de l'API REST du Centre de contrôle	44
7 Options de configuration supplémentaires	46
Reconfiguration de l'authentification	46
Modifier le fournisseur d'authentification	46
Modifier les paramètres d'authentification	47
Exporter la configuration Orchestrator	48
Importer la configuration d'Orchestrator	49
Configuration des propriétés d'exécution de workflow	49
Fichiers journaux d'Orchestrator	50
Permanence des consignations	51
Configuration des journaux d'Orchestrator	52
Filtrer les journaux d'Orchestrator	52
Configuration de l'intégration de la journalisation avec le serveur distant	53
Ajouter des cartes réseau	54
Configurer des itinéraires statiques	55
8 Cas d'utilisation de configuration et dépannage	56
Configurer le plug-in vRealize Orchestrator pour vSphere Web Client	56
Annuler l'enregistrement de l'authentification Orchestrator	57
Modification des certificats SSL	58

Ajout d'un certificat au magasin local	58
Modifier le certificat du site de gestion du dispositif Orchestrator Appliance	59
Annuler des workflows en cours d'exécution	59
Permettre le débogage du serveur Orchestrator	60
Sauvegarder les éléments et la configuration de Orchestrator	61
Sauvegarde et restauration de vRealize Orchestrator	64
Sauvegarder vRealize Orchestrator	64
Restaurer une instance de vRealize Orchestrator	65
Récupération d'urgence d'Orchestrator à l'aide de Site Recovery Manager	66
Configurer des machines virtuelles pour vSphere Replication	67
Créer des groupes de protection	67
Créer un plan de récupération	68
Organiser des plans de récupération dans des dossiers	69
Modifier un plan de récupération	70
9 Configuration des propriétés du système	71
Désactiver l'accès au client Orchestrator pour les non-administrateurs	71
Configuration de l'accès au système de fichiers du serveur pour les workflows et les actions	72
Règles dans le fichier js-io-rights.conf autorisant l'accès en écriture au système Orchestrator	72
Configurer l'accès au système de fichiers du serveur pour les workflows et les actions	73
Définir l'accès aux commandes du système d'exploitation pour les workflows et les actions	74
Définir l'accès du JavaScript aux classes Java	75
Définir la propriété de délai d'expiration personnalisée	76
10 Pour aller plus loin	78
Se connecter au client Orchestrator à partir de la console Web du dispositif Orchestrator	78

Installation et configuration de VMware vRealize Orchestrator

Le chapitre *Installation et configuration VMware vRealize Orchestrator* fournit des informations et des instructions concernant l'installation, la mise à niveau et la configuration de VMware[®] vRealize Orchestrator.

Public cible

Ces informations s'adressent à des administrateurs vSphere avancés et 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](#)
- [Types d'utilisateurs d'Orchestrator et responsabilités associées](#)
- [Architecture d'Orchestrator](#)
- [Plug-ins Orchestrator](#)

Fonctionnalités clés de la plate-forme Orchestrator

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. Orchestrator est une plate-forme ouverte avec des capacités d'extension aux nouveaux plug-ins et bibliothèques et peut être intégré à des architectures plus vastes via une API REST.

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

Persistance

Des bases de données de niveau production sont utilisées pour stocker des informations pertinentes (comme des processus, des états des workflows et la configuration d'Orchestrator).

Gestion centralisée

Avec 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 vRealize Orchestrator en proposant une interface d'administration centralisée pour les opérations en cours d'exécution, la surveillance des workflows, l'accès unifié au journal et ses configurations, ainsi que la corrélation entre les workflows qui s'exécutent et les ressources du système. Le mécanisme de journalisation d'Orchestrator est optimisé par un fichier journal complémentaire qui agrège diverses mesures de performances pour le débit du moteur d'Orchestrator.

Contrôle de version

Tous les objets de la plate-forme 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.

Moteur de scripts

Le moteur JavaScript Mozilla Rhino procure un moyen de créer des blocs constitutifs pour la plate-forme Orchestrator. 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 actions qu'Orchestrator propose
- Les blocs constitutifs personnalisés créés par le client
- Les objets que les plug-ins ajoutent à Orchestrator

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 Orchestrator 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.

Client de surveillance

Surveillez les processus d'Orchestrator via le client de surveillance de l'interface utilisateur Web. Vous pouvez utiliser ces informations pour dépanner les processus d'Orchestrator.

Développement et ressources

La page de lancement d'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 d'Orchestrator pour envoyer des demandes au serveur Orchestrator.

Sécurité

Orchestrator offre les fonctions de sécurité avancée 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.
- Un mécanisme SSL (Secure Sockets Layer) pour assurer le chiffrement des communications entre le client du poste de travail et le serveur, et un accès en 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.

Types d'utilisateurs d'Orchestrator et responsabilités associées

Orchestrator propose différents outils et interfaces en fonction des responsabilités particulières des rôles d'utilisateurs globaux. Dans Orchestrator, vous pouvez avoir des utilisateurs pourvus de droits complets, qui font partie du groupe d'administration (ci-après, les Administrateurs) et des utilisateurs aux droits limités, qui ne font pas partie du groupe d'administration (à savoir, les Utilisateurs finals).

Utilisateurs aux droits complets

Les administrateurs et développeurs d'Orchestrator disposent des mêmes droits d'administration, mais ne partagent pas les mêmes responsabilités.

Administrateurs

Ce rôle dispose d'un accès complet à l'ensemble des fonctionnalités de la plate-forme Orchestrator. Les responsabilités de base de l'administration se composent de :

- L'installation et la configuration d'Orchestrator
- La gestion des droits d'accès à Orchestrator et aux applications
- Importation et exportation de modules
- L'exécution des workflows et la planification des tâches
- La gestion du contrôle de version des éléments importés
- La création de nouveaux workflows et plug-ins

Développeurs

Ce type d'utilisateur a un accès complet à l'ensemble des fonctionnalités de la plate-forme Orchestrator. Développeurs se voient accorder l'accès à l'interface du client Orchestrator et disposent des fonctionnalités suivantes :

- Création d'applications pour étendre la fonctionnalité de la plate-forme Orchestrator
- L'automatisation des processus par la personnalisation des workflows existants et la création de nouveaux workflows et plug-ins

Utilisateurs aux droits limités

Utilisateurs finals

Les utilisateurs finals ont la possibilité d'exécuter et de planifier des workflows et des stratégies que les administrateurs ou les développeurs rendent disponibles dans le client Orchestrator.

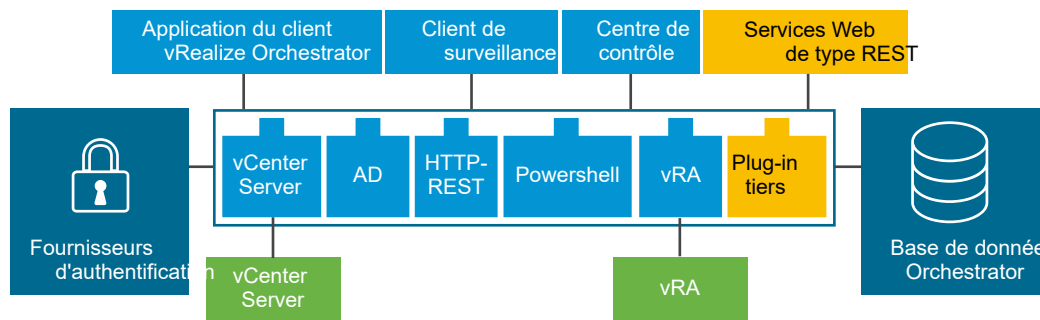
Architecture d'Orchestrator

Orchestrator contient une bibliothèque de workflows et un moteur de workflow qui vous permet de créer et d'exécuter des workflows automatisant les processus d'orchestration. Vous exécutez les workflows sur les objets des différentes technologies auxquelles Orchestrator accède au travers d'une série de plug-ins.

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

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. Orchestrator est relié à un fournisseur d'authentification pour la gestion des comptes utilisateurs et à une base de données pour le stockage des informations issues des workflows qu'il exécute. Vous pouvez accéder à Orchestrator, aux objets qu'il expose et aux workflows d'Orchestrator via l'interface du client Orchestrator ou via les services Web. La surveillance et la configuration des services et des workflows d'Orchestrator s'effectuent via le client de surveillance et le Centre de contrôle.

Figure 1-1. Architecture de VMware vRealize Orchestrator



Plug-ins Orchestrator

Les plug-ins vous permettent d'utiliser Orchestrator pour accéder à des technologies et à des applications externes, et pour les contrôler. En exposant une technologie externe dans un plug-in 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.

Orchestrator fournit un ensemble de plug-ins standard que vous pouvez utiliser pour intégrer des technologies telles que les API vCenter Server VMware 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 vRealize Automation et des services applicatifs existants. Vous pouvez également utiliser l'architecture modulaire ouverte d'Orchestrator pour développer des plug-ins afin d'accéder à d'autres applications.

Les plug-ins Orchestrator développés par VMware sont distribués sous forme de fichiers `.vmoapp`. Pour en savoir plus sur les plug-ins Orchestrator développés et distribués par VMware, consultez les [Plug-ins externes de vRealize Orchestrator](#). Pour en savoir plus sur les plug-ins Orchestrator tiers, reportez-vous à [VMware Solution Exchange](#).

Configuration requise du système pour Orchestrator

2

Votre système doit satisfaire aux conditions requises techniques qui sont nécessaires au fonctionnement correct d'Orchestrator.

Pour connaître la liste des versions prises en charge de vCenter Server, vSphere Web Client, vRealize Automation et des autres solutions VMware, ainsi que des versions de bases de données compatibles, consultez la [Matrice d'interopérabilité des produits VMware](#).

Ce chapitre contient les rubriques suivantes :

- [Configuration matérielle requise pour le dispositif Orchestrator Appliance](#)
- [Navigateurs pris en charge par Orchestrator](#)
- [Configuration requise pour la base de données d'Orchestrator](#)
- [Logiciel inclus dans le dispositif Orchestrator Appliance](#)
- [Niveau de prise en charge de l'internationalisation](#)
- [Ports réseau d'Orchestrator](#)

Configuration matérielle requise pour le dispositif Orchestrator Appliance

Le Orchestrator Appliance est une machine virtuelle basée sur Linux préconfigurée. Avant de déployer le dispositif, vérifiez que votre système dispose de la configuration matérielle minimale requise.

Le dispositif Orchestrator Appliance nécessite la configuration matérielle suivante :

- 2 CPU
- 6 Go de mémoire
- 17 Go de disque dur

Ne réduisez pas la taille de la mémoire par défaut, car le serveur Orchestrator nécessite au moins 2 Go de mémoire libre.

Navigateurs pris en charge par Orchestrator

Le Centre de contrôle nécessite un navigateur Web.

Vous devez utiliser l'un des navigateurs suivants pour vous connecter au Centre de contrôle.

- Microsoft Edge
- Mozilla Firefox
- Google Chrome

Configuration requise pour la base de données d'Orchestrator

Le serveur Orchestrator inclut une base de données PostgreSQL préconfigurée prête pour la production.

À partir de vRealize Orchestrator 7.5, l'intégration de la base de données externe n'est pas prise en charge. Vous pouvez uniquement utiliser la base de données PostgreSQL préconfigurée.

Logiciel inclus dans le dispositif Orchestrator Appliance

Le dispositif Orchestrator Appliance est une machine virtuelle préconfigurée, optimisée pour l'exécution d'Orchestrator. Le dispositif est distribué avec un logiciel préinstallé.

Le module Orchestrator Appliance contient le logiciel suivant :

- SUSE Linux Enterprise Server 11 Update 3 pour VMware, édition 64 bits
- PostgreSQL
- Orchestrator

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

Note Pour utiliser le dispositif Orchestrator Appliance dans un environnement de production, vous devez configurer le serveur Orchestrator pour s'authentifier via vRealize Automation ou vSphere. Pour plus d'informations sur la configuration d'un fournisseur d'authentification, reportez-vous à la section [Configuration d'un serveur Orchestrator autonome](#).

Niveau de prise en charge de l'internationalisation

Le centre de contrôle Orchestrator inclut les langues suivantes : espagnol, français, allemand, chinois traditionnel, chinois simplifié, coréen et japonais. Le client Orchestrator prend en charge l'internationalisation de niveau 1.

Prise en charge des caractères non-ASCII dans Orchestrator

Bien que le client Orchestrator ne soit pas localisé, il peut être exécuté sur des systèmes d'exploitation non anglais et prendre en charge le texte non-ASCII.

Tableau 2-1. Prise en charge des caractères non-ASCII dans l'interface utilisateur d'Orchestrator

Prise en charge des caractères non-ASCII				
Élément Orchestrator	Champ Description	Champ Nom	Paramètres d'entrée et de sortie	Attributs
Action	Oui	Non	Non	Non
Dossier	Oui	Oui	-	-
Élément de configuration	Oui	Oui	-	Non
Module	Oui	Oui	-	-
Stratégie	Oui	Oui	-	-
Modèle de stratégie	Oui	Oui	-	-
Élément de ressource	Oui	Oui	-	-
Workflow	Oui	Oui	Non	Non
Groupe d'affichage de présentation de workflow et étape d'entrée	Oui	Oui	-	-

Ports réseau d'Orchestrator

Orchestrator se sert de ports précis pour communiquer avec les autres systèmes. Ces ports sont définis sur une valeur par défaut qu'il est impossible de modifier.

Ports de configuration par défaut

Pour proposer un service Orchestrator, vous devez définir des ports par défaut et configurer votre pare-feu pour qu'il autorise les communications TCP entrantes.

Note D'autres ports peuvent s'avérer indispensables si vous utilisez des plug-ins personnalisés.

Tableau 2-2. Ports de configuration par défaut de VMware vRealize Orchestrator

Port	Numéro	Protocole	Source	Cible	Description
Interface de gestion du dispositif virtuel	5480	TCP			Le port d'accès à l'interface des paramètres système du dispositif.
port du serveur HTTP	8280	TCP	Navigateur Web de l'utilisateur	Serveur Orchestrator	Les demandes adressées au port Web HTTP par défaut d'Orchestrator (8280) sont redirigées vers son port Web HTTPS par défaut (8281).

Tableau 2-2. Ports de configuration par défaut de VMware vRealize Orchestrator (suite)

Port	Numéro	Protocole	Source	Cible	Description
port du serveur HTTPS	8281	TCP	Navigateur Web de l'utilisateur	Serveur Orchestrator	Port d'accès pour la page d'accueil Web d'Orchestrator.
port d'accès HTTPS pour la configuration Web	8283	TCP	Navigateur Web de l'utilisateur	Configuration d'Orchestrator	Port d'accès SSL pour l'UI Web de configuration d'Orchestrator.

Ports de communication externe

Vous devez configurer votre pare-feu pour qu'il autorise les connexions sortantes de telle sorte qu'Orchestrator puisse communiquer avec des services externes.

Tableau 2-3. Ports de communication externe de VMware vRealize Orchestrator

Port	Numéro	Protocole	Source	Cible	Description
PostgreSQL	5432	TCP	Serveur Orchestrator	PostgreSQL Server	C'est le port servant à communiquer avec PostgreSQL Server qui est configuré en tant que base de données d'Orchestrator.
port du serveur SMTP	25	TCP	Serveur Orchestrator	Serveur SMTP	C'est le port employé pour les notifications par e-mail.
Port de l'API vCenter Server	443	TCP	Serveur Orchestrator	vCenter Server	C'est le port de communication de l'API vCenter Server employé par Orchestrator pour obtenir les informations d'infrastructure virtuelle et de machines virtuelles auprès des instances orchestrées de vCenter Server.

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.
- Pour les environnements vRealize Orchestrator en cluster, installez un serveur d'équilibrage de charge et configurez-le afin de distribuer la charge de travail entre deux ou plusieurs serveurs vRealize Orchestrator.

Ce chapitre contient les rubriques suivantes :

- [Configuration de vCenter Server](#)
- [Méthodes d'authentification](#)

Configuration de vCenter Server

L'augmentation du nombre d'instances vCenter Server dans votre configuration d'Orchestrator pousse ce dernier à gérer des sessions supplémentaires. Trop de sessions actives peuvent entraîner des délais d'expiration d'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 Vous pouvez exécuter plusieurs instances vCenter Server sur différentes machines virtuelles dans votre configuration Orchestrator si votre réseau dispose de suffisamment de bande passante et de latence. Si vous utilisez le LAN pour améliorer la communication entre Orchestrator et vCenter Server, une ligne de 100 Mo est obligatoire.

Méthodes d'authentification

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

Lorsque vous téléchargez et déployez le dispositif Orchestrator Appliance, vous devez configurer une connexion avec vRealize Automation ou vSphere.

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](#)

Télécharger et déployer le dispositif vRealize Orchestrator Appliance

Téléchargez et installez un dispositif vRealize Orchestrator Appliance en le déployant à partir d'un modèle.

Conditions préalables

- Vérifiez que vCenter Server est installé et en cours d'exécution.
- Vérifiez que l'hôte sur lequel vous déployez le dispositif vRealize Orchestrator Appliance répond à la configuration matérielle minimale. Pour plus d'informations, reportez-vous à la section [Configuration matérielle requise pour le dispositif 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 Dans vSphere Web Client, sélectionnez un objet d'inventaire qui est 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 déployé.

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 (Facultatif) Configurez les paramètres réseau et cliquez sur **Suivant**.

Par défaut, le vRealize Orchestrator Appliance utilise DHCP. Vous pouvez modifier ce paramètre et attribuer une adresse IP fixe à partir de la console Web du dispositif.

- 12 Sélectionnez les options que vous souhaitez activer et définissez le mot de passe initial pour le compte d'utilisateur racine.

Votre mot de passe initial doit comporter au moins huit caractères.

Important Le mot de passe du compte racine du dispositif Orchestrator Appliance expire après 365 jours. Si vous souhaitez augmenter le délai d'expiration d'un compte, connectez-vous au dispositif Orchestrator Appliance en tant que racine et exécutez `passwd -x number_of_days name_of_account`. Si vous souhaitez augmenter le délai du mot de passe racine du dispositif Orchestrator Appliance jusqu'à l'infini, exécutez la commande `passwd -x 99999 root`.

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

Résultats

Le vRealize Orchestrator Appliance est correctement déployé.

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

Pour utiliser le dispositif vRealize Orchestrator Appliance, vous devez d'abord le mettre sous tension, puis obtenir une adresse IP pour le dispositif virtuel.

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 Une fois le dispositif mis sous tension, sélectionnez l'onglet **Résumé** pour afficher l'adresse IP du dispositif vRealize Orchestrator Appliance.
- 4 Dans un navigateur Web, accédez à l'adresse d'hôte de la machine virtuelle de votre dispositif vRealize Orchestrator Appliance.

`https://votre_nom_d'hôte_orchestrator/vco.`

Modifier le mot de passe racine

Pour des raisons de sécurité, modifiez le mot de passe du dispositif vRealize Orchestrator Appliance.

Par défaut, le mot de passe du compte racine du dispositif vRealize Orchestrator Appliance expire après 365 jours. Vous pouvez augmenter le délai d'expiration du compte racine en vous connectant au dispositif vRealize Orchestrator Appliance via un client SSH et en exécutant `passwd -x nombre_de_jours nom_du_compte`. Si vous souhaitez augmenter le mot de passe racine du dispositif vRealize Orchestrator Appliance jusqu'à un délai infini, exécutez `passwd -x 99999 root`.

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 l'interface VAMI de vRealize Orchestrator en tant que **racine**.
Accédez à l'interface VAMI à l'adresse `https://votre_nom_d'hôte_orchestrator:5480`.
- 2 Sélectionnez l'onglet **Admin**.
- 3 Dans la zone de texte **Mot de passe d'administrateur actuel**, entrez le mot de passe racine actuel.

- 4 Entrez le nouveau mot de passe dans les zones de texte **Nouveau mot de passe administrateur** et **Confirmer le nouveau mot de passe administrateur**.
- 5 Cliquez sur **Enregistrer les paramètres**.

Résultats

Le mot de passe de l'utilisateur Linux racine du dispositif vRealize Orchestrator Appliance a été correctement modifié.

Activer ou désactiver la connexion administrateur SSH sur le 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 l'interface VAMI de vRealize Orchestrator en tant que **racine**.
Accédez à l'interface VAMI à l'adresse `https://votre_nom_d'hôte_orchestrator:5480`.
- 2 Dans l'onglet **Admin**, cliquez sur **Service SSH activé** pour activer ou désactiver le service SSH de vRealize Orchestrator.
- 3 (Facultatif) Cliquez sur **Connexion SSH de l'administrateur activée** pour activer ou désactiver l'accès racine au dispositif vRealize Orchestrator Appliance via SSH.
- 4 Cliquez sur **Enregistrer les paramètres**.

Résultats

Lorsque ce paramètre est activé, l'**État SSH** apparaît comme *En cours d'exécution*. Lorsqu'il est désactivé, l'**État SSH** apparaît comme *Arrêté*.

Configurer les paramètres réseau du dispositif vRealize Orchestrator Appliance

Configurez les paramètres réseau du dispositif vRealize Orchestrator Appliance pour attribuer une adresse IP statique et définir les paramètres de proxy.

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 l'interface VAMI de vRealize Orchestrator en tant que **racine**.
Accédez à l'interface VAMI à l'adresse `https://votre_nom_d'hôte_orchestrator:5480`.
- 2 Dans l'onglet **Réseau**, cliquez sur **Adresse**.
- 3 Sélectionnez la méthode qu'utilisera le dispositif vRealize Orchestrator Appliance pour obtenir les paramètres d'adresse IP.

Option	Description
DHCP	Permet d'obtenir les paramètres IP à partir d'un serveur DHCP. Il s'agit du paramètre par défaut.
Statique	Utilise des paramètres IP statiques Si vous sélectionnez cette option, le système vous invite à entrer une adresse IP, un masque réseau (pour IPv4), un préfixe (pour IPv6) et des informations de passerelle.

Selon vos paramètres réseau, vous devrez peut-être sélectionner des types d'adresses IPv4 et IPv6.

- 4 Cliquez sur **Enregistrer les paramètres**.
- 5 (Facultatif) Pour configurer un serveur proxy, sélectionnez l'onglet **Proxy**.
- 6 (Facultatif) Après avoir configuré vos paramètres de proxy, cliquez sur **Enregistrer les paramètres**.

Configuration initiale

5

Avant de commencer à automatiser des tâches et à gérer des systèmes et des applications avec Orchestrator, vous devez le configurer pour utiliser un fournisseur d'authentification externe et attribuer des rôles à différents utilisateurs. Vous pouvez également importer des certificats signés par une autorité de certification, installer des plug-ins ou modifier la configuration des journaux par défaut.

Ce chapitre contient les rubriques suivantes :

- [Configuration d'un serveur Orchestrator autonome](#)
- [Ports réseau d'Orchestrator](#)
- [Connexion à la base de données Orchestrator](#)
- [Gérer les certificats](#)
- [Configurer les plug-ins Orchestrator](#)
- [Disponibilité et évolutivité d'Orchestrator](#)
- [Configuration du programme d'amélioration du produit](#)

Configuration d'un serveur Orchestrator autonome

Bien que le dispositif Orchestrator Appliance soit une machine virtuelle basée sur Linux préconfigurée, vous devez suivre l'assistant de configuration avant d'accéder au centre de contrôle Orchestrator.

Configurer un serveur Orchestrator autonome avec l'authentification vRealize Automation

Pour préparer le dispositif Orchestrator Appliance, vous devez configurer les paramètres de l'hôte et le fournisseur d'authentification. Vous pouvez configurer Orchestrator pour utiliser l'authentification via le registre de composants vRealize Automation.

Conditions préalables

- Téléchargez et déployez la dernière version du dispositif vRealize Orchestrator. Reportez-vous à la section [Télécharger et déployer le dispositif vRealize Orchestrator Appliance](#).

- Installez et configurez vRealize Automation, puis vérifiez que votre serveur vRealize Automation est en cours d'exécution. Consultez la documentation de vRealize Automation.

Si vous prévoyez de créer un cluster :

- Configurez un équilibrage de charge pour distribuer le trafic entre plusieurs instances de vRealize Orchestrator. Pour plus d'informations, reportez-vous à la documentation relative à l'équilibrage de charge vRealize Orchestrator.

Procédure

- 1 Accédez au centre de contrôle pour démarrer l'assistant de configuration.
 - a Accédez à `https://IP_de_votre_serveur_orchestrator_ou_nom_DNS:8283/vco-controlcenter`.
 - b Connectez-vous en tant que **root** avec le mot de passe que vous avez entré lors du déploiement OVA.
- 2 Cliquez sur **MODIFIER** pour configurer le nom d'hôte sur lequel le centre de contrôle sera accessible.

Note Si vous êtes sur le point de configurer un cluster Orchestrator, entrez le nom d'hôte du serveur virtuel d'équilibrage de charge.

- 3 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**.
 - c Cliquez sur **Accepter le certificat**.
 - d Dans les zones de texte **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification du compte d'utilisateur configuré pour la connexion SSO dans vRealize Automation. Cliquez sur **ENREGISTRER**.

Par défaut, le compte SSO est **administrateur** 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\vcadmins**
 - f Dans la liste des groupes, double-cliquez sur le nom du groupe pour le sélectionner.
 - g Cliquez sur **ENREGISTRER LES MODIFICATIONS**.

Un message indique la réussite de l'enregistrement, et vous êtes redirigé vers la vue principale du centre de contrôle.

Résultats

Vous avez terminé la configuration du Centre de contrôle.

Étape suivante

- Vérifiez que **VRA** 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 Orchestrator redémarre automatiquement après 2 minutes. Une vérification de la configuration immédiatement après l'achèvement du processus peut renvoyer un état de configuration non valide.

Configurer un serveur Orchestrator autonome avec l'authentification vSphere

Vous enregistrez le serveur 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. Reportez-vous à la section [Télécharger et déployer le dispositif vRealize Orchestrator Appliance](#).
- Installez et configurez vCenter Server avec le serveur vCenter Single Sign-On en cours d'exécution. Pour plus d'informations, consultez la documentation vSphere.

Si vous prévoyez de créer un cluster :

- Configurez un équilibrage de charge pour distribuer le trafic entre plusieurs instances de vRealize Orchestrator. Pour plus d'informations, reportez-vous à la documentation relative à l'équilibrage de charge vRealize Orchestrator.

Procédure

- 1 Accédez au centre de contrôle pour démarrer l'assistant de configuration.
 - a Accédez à `https://IP_de_votre_serveur_orchestrator_ou_nom_DNS:8283/vco-controlcenter`.
 - b Connectez-vous en tant que **root** avec le mot de passe que vous avez entré lors du déploiement OVA.
- 2 Cliquez sur **MODIFIER** pour configurer le nom d'hôte sur lequel le centre de contrôle sera accessible.

Note Si vous êtes sur le point de configurer un cluster Orchestrator, entrez le nom d'hôte du serveur virtuel d'équilibrage de charge.

3 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 dans Orchestrator les certificats de toutes les instances de Platform Services Controller qui partagent le même domaine vCenter Single Sign-On.

- c Cliquez sur **Accepter le certificat**.
- d Dans les zones de texte **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification du compte 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 Dans la liste des groupes, double-cliquez sur le nom du groupe pour le sélectionner.
- g Cliquez sur **ENREGISTRER LES MODIFICATIONS**.

Un message indique la réussite de l'enregistrement, et vous êtes redirigé vers la vue principale du centre de contrôle.

Résultats

Vous avez terminé la configuration du centre de contrôle.

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 Orchestrator redémarre automatiquement après 2 minutes. Une vérification de la configuration immédiatement après l'achèvement du processus peut renvoyer un état de configuration non valide.

Ports réseau d'Orchestrator

Orchestrator se sert de ports précis pour communiquer avec les autres systèmes. Ces ports sont définis sur une valeur par défaut qu'il est impossible de modifier.

Ports de configuration par défaut

Pour proposer un service Orchestrator, vous devez définir des ports par défaut et configurer votre pare-feu pour qu'il autorise les communications TCP entrantes.

Note D'autres ports peuvent s'avérer indispensables si vous utilisez des plug-ins personnalisés.

Tableau 5-1. Ports de configuration par défaut de VMware vRealize Orchestrator

Port	Numéro	Protocole	Source	Cible	Description
Interface de gestion du dispositif virtuel	5480	TCP			Le port d'accès à l'interface des paramètres système du dispositif.
port du serveur HTTP	8280	TCP	Navigateur Web de l'utilisateur	Serveur Orchestrator	Les demandes adressées au port Web HTTP par défaut d'Orchestrator (8280) sont redirigées vers son port Web HTTPS par défaut (8281).
port du serveur HTTPS	8281	TCP	Navigateur Web de l'utilisateur	Serveur Orchestrator	Port d'accès pour la page d'accueil Web d'Orchestrator.
port d'accès HTTPS pour la configuration Web	8283	TCP	Navigateur Web de l'utilisateur	Configuration d'Orchestrator	Port d'accès SSL pour l'UI Web de configuration d'Orchestrator.

Ports de communication externe

Vous devez configurer votre pare-feu pour qu'il autorise les connexions sortantes de telle sorte qu'Orchestrator puisse communiquer avec des services externes.

Tableau 5-2. Ports de communication externe de VMware vRealize Orchestrator

Port	Numéro	Protocole	Source	Cible	Description
PostgreSQL	5432	TCP	Serveur Orchestrator	PostgreSQL Server	C'est le port servant à communiquer avec PostgreSQL Server qui est configuré en tant que base de données d'Orchestrator.
port du serveur SMTP	25	TCP	Serveur Orchestrator	Serveur SMTP	C'est le port employé pour les notifications par e-mail.
Port de l'API vCenter Server	443	TCP	Serveur Orchestrator	vCenter Server	C'est le port de communication de l'API vCenter Server employé par Orchestrator pour obtenir les informations d'infrastructure virtuelle et de machines virtuelles auprès des instances orchestrées de vCenter Server.

Connexion à la base de données Orchestrator

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

Lorsque vous téléchargez et déployez Orchestrator Appliance, le serveur Orchestrator est configuré pour fonctionner avec la base de données PostgreSQL préinstallée dans le dispositif.

La base de données PostgreSQL d'Orchestrator préconfigurée est prête pour la production. Toutes les transactions de la base de données PostgreSQL d'Orchestrator sont gérées automatiquement via l'interface VAMI.

Note À partir de vRealize Orchestrator 7.5, les bases de données externes comme Oracle et Microsoft SQL ne sont pas prises en charge.

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 non votre signature est digne de confiance.

■ Gérer les certificats Orchestrator

Vous pouvez gérer les certificats Orchestrator depuis la page **Certificats** dans le Centre de contrôle ou via le client Orchestrator, en utilisant les workflows Gestionnaire de confiance SSL de la catégorie de workflow Configuration.

Gérer les certificats Orchestrator

Vous pouvez gérer les certificats Orchestrator depuis la page **Certificats** dans le Centre de contrôle ou via le client Orchestrator, en utilisant les workflows Gestionnaire de confiance SSL de la catégorie de workflow Configuration.

Importer un certificat dans un magasin de confiance d'Orchestrator

Le Centre de contrôle 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 SSL requis d'une URL ou d'un fichier codé PEM. Chaque fois que vous utilisez une connexion SSL 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 SSL correspondant.

Vous pouvez charger le certificat SSL dans 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 : <code>https://adresse_IP_de_votre_serveur</code> ou <code>adresse_IP_de_votre_serveur:port</code>
Importer à partir d'un fichier	Chemin d'accès au fichier de certificat codé PEM. Pour plus d'informations sur l'importation d'un fichier de certificat codé PEM, reportez-vous à la section Importer un certificat de confiance via le centre de contrôle .

Générer un certificat de serveur autosigné

Le Orchestrator Appliance inclut un certificat autosigné généré automatiquement, basé sur les paramètres réseau du dispositif. Si les paramètres réseau du dispositif sont modifiés, vous devez générer manuellement un nouveau certificat autosigné. Vous pouvez créer un certificat autosigné pour garantir une communication chiffrée et fournir une signature pour vos modules. Toutefois, le destinataire ne peut pas être sûr que le module autosigné 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.

Vous pouvez générer un certificat autosigné sous l'onglet **Certificat SSL de serveur Orchestrator** de la page **Certificats** dans le Centre de contrôle.

Option	Description
Algorithme de signature	Algorithme de chiffrement permettant de générer une signature numérique.
Nom commun	Nom d'hôte du serveur Orchestrator.
Organisation	Nom de votre organisation. Par exemple, VMware .
Unité d'organisation	Nom de votre unité d'organisation. Par exemple, R&D .
Code pays	Abréviation du code pays. Par exemple, US .

Orchestrator génère un certificat de serveur unique pour votre environnement. Les détails de la clé publique du certificat s'affichent dans l'onglet **Certificat SSL de serveur Orchestrator**. La clé privée est stockée dans la table `vmo_keystore` de la base de données Orchestrator.

Importer un certificat SSL de serveur Orchestrator

vRealize Orchestrator utilise un certificat SSL pour s'identifier auprès des clients et des serveurs distants lors d'une communication sécurisée. Par défaut, Orchestrator inclut un certificat SSL autosigné généré automatiquement, basé sur les paramètres réseau du dispositif. Vous pouvez importer un certificat SSL signé par une autorité de certification pour éviter les erreurs de confiance de certificats.

Vous devez importer un certificat signé par une autorité de certification sous forme de fichier codé PEM contenant les clés publique et privée.

Note Après la génération ou l'importation d'un certificat de serveur SSL, redémarrez le service Orchestrator Configurator.

```
service vco-configurator restart
```

Certificat de signature de module

Les modules exportés à partir d'un serveur 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 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.

Note Le dispositif Orchestrator Appliance inclut un certificat de module autosigné généré automatiquement lors de la configuration initiale d'Orchestrator. Vous pouvez modifier le certificat de signature de module, après quoi tous les modules exportés ultérieurement sont signés avec le nouveau certificat.

Importer un certificat de confiance via le centre de contrôle

Pour communiquer en toute sécurité avec les autres serveurs, le serveur Orchestrator doit pouvoir vérifier leur identité. Pour cela, vous devrez peut-être importer le certificat SSL de l'entité distante dans le magasin de confiance d'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.

Conditions préalables

Recherchez le nom de domaine complet du serveur auquel vous voulez qu'Orchestrator se connecte via SSL.

Procédure

- 1 Connectez-vous au dispositif Orchestrator Appliance sur SSH en tant que **racine**.
- 2 Exécutez une commande pour récupérer le certificat du serveur distant.

```
openssl s_client -connect host_or_dns_name:secure_port
```

- a Si vous utilisez un port non chiffré, utilisez `starttls` et le protocole requis avec la commande `openssl`.

```
openssl s_client -connect nom_hôte_ou_dns:port -starttls smtp
```

- 3 Copiez le texte compris entre les balises `-----BEGIN CERTIFICATE-----` et `-----END CERTIFICATE-----` dans un éditeur de texte et enregistrez-le en tant que fichier.
- 4 Connectez-vous au centre de contrôle en tant que **root**.
- 5 Accédez à la page **Certificats**.

- 6 Dans l'onglet **Certificats de confiance**, cliquez sur **Importer** et sélectionnez l'option **Importer à partir d'un fichier codé PEM**.
- 7 Accédez au fichier de certificat et cliquez sur **Importer**.

Résultats

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

Configurer les plug-ins Orchestrator

Les plug-ins Orchestrator par défaut sont configurés uniquement via des workflows.

Si vous souhaitez configurer des plug-ins Orchestrator par défaut, vous devez utiliser le workflow spécifique du client Orchestrator.

Gérer les plug-Ins vRealize Orchestrator

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

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.

Installer ou mettre à niveau un nouveau plug-in

Les plug-ins vRealize Orchestrator permettent au serveur vRealize Orchestrator de s'intégrer à d'autres produits logiciels. Le dispositif vRealize Orchestrator Appliance inclut un ensemble de plug-ins 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. Les extensions de fichier à utiliser sont `.vmoapp` et `.dar`. Un fichier `.vmoapp` peut contenir une collection de plusieurs fichiers `.dar` et peut être installé en tant qu'application. Un fichier `.dar` contient toutes les ressources associées à un plug-in.

Note Le format de fichier recommandé pour les plug-ins vRealize Orchestrator 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](#).

Désactiver un plug-in

Vous pouvez désactiver un plug-in en désactivant la case **Activer** 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 Orchestrator, reportez-vous à [Désinstaller un plug-in](#).

Installer ou mettre à jour un plug-in vRealize Orchestrator

Vous pouvez installer ou mettre à jour des plug-ins tiers avec 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**.

Désinstaller un plug-in

Vous pouvez utiliser le centre de contrôle pour supprimer un plug-in, mais cette action ne supprime pas tout son contenu de votre environnement vRealize Orchestrator. Après la suppression du plug-in du centre de contrôle, vous devez supprimer les modules et les dossiers de plug-in associés du client vRealize Orchestrator.

Procédure

- 1 Supprimez le plug-in du centre de contrôle Orchestrator.
 - a Connectez-vous au centre de contrôle en tant qu'utilisateur **racine**.
 - b Sélectionnez **Gérer les plug-ins**.
 - c Trouvez le plug-in que vous souhaitez supprimer, puis cliquez sur l'icône Supprimer.
 - d Cliquez sur **Supprimer**.

2 Supprimer les modules et les dossiers du plug-in du client vRealize Orchestrator.

- a Connectez-vous au client vRealize Orchestrator.
- b Sélectionnez **Conception** dans le menu déroulant situé dans le coin supérieur gauche.
- c Sélectionnez l'onglet **Modules**.
- d Cliquez avec le bouton droit sur le module que vous souhaitez supprimer, puis sélectionnez **Supprimer un élément avec du contenu**.

Note Pour supprimer tout le contenu du plug-in, y compris le contenu personnalisé partagé, sélectionnez **Supprimer tout**. Pour préserver le contenu personnalisé que le module du plug-in partage avec d'autres objets vRealize Orchestrator, sélectionnez **Conserver les modules partagés**. Le contenu vRealize Orchestrator verrouillé en lecture seule, tel que les workflows de la bibliothèque standard, n'est pas supprimé, quelle que soit l'option sélectionnée.

- e Sélectionnez l'onglet **Workflow**.
- f Développez la bibliothèque de workflows et supprimez le dossier du plug-in que vous souhaitez supprimer.
- g Sélectionnez l'onglet **Actions**.
- h Supprimez les modules d'action du plug-in que vous voulez effacer.

3 Redémarrez les services vRealize Orchestrator.

```
service vco-configurator restart && service vco-server restart
```

Résultats

Vous avez désinstallé le plug-in et son contenu de votre environnement vRealize Orchestrator.

Disponibilité et évolutivité d'Orchestrator

Pour augmenter la disponibilité des services Orchestrator, démarrez plusieurs instances de serveur 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.

Cluster Orchestrator

Les instances de serveur 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 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 Orchestrator qui cesse de répondre. Si une instance de serveur 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 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.

Orchestrator ne fournit pas d'outil intégré pour surveiller l'état du cluster et envoyer des notifications de basculement. Vous pouvez surveiller l'état du cluster à l'aide d'un composant externe tel qu'un équilibreur de charge. Pour vérifier si un nœud est en cours d'exécution, vous pouvez utiliser le service d'API REST d'état d'intégrité à l'adresse https://IP_de_votre_serveur_orchestrator_ou_nom_DNS:8281/vco/api/healthstatus et vérifier l'état du nœud ou à l'adresse https://IP_de_votre_serveur_orchestrator_ou_nom_DNS:8283/vco-controlcenter/docs/ pour surveiller l'état du centre de contrôle.

Configurer un cluster d'instances de vRealize Orchestrator dans l'interface VAMI

À partir de vRealize Orchestrator 7.5, toutes les opérations de clustering sont effectuées via l'interface VAMI d'Orchestrator Appliance.

Un cluster Orchestrator se compose d'au moins deux instances d'Orchestrator qui partagent une base de données. Configurez un nouveau cluster Orchestrator ou ajoutez de nouveaux nœuds à un cluster existant à partir de l'interface VAMI d'Orchestrator. Il existe trois types de nœuds dans le cluster Orchestrator.

Type de nœud	Définition
Nœud principal	Chaque cluster Orchestrator dispose d'un seul nœud principal. Tous les nœuds du cluster partagent la base de données PostgreSQL du nœud principal. La base de données principale peut s'exécuter en mode synchrone et asynchrone. Le nœud principal doit être dans un état sain pour que le cluster fonctionne.
Nœud de réplica	Les nœuds de réplica sont des instances d'Orchestrator jointes au nœud Orchestrator principal.
Nœud de réplica synchronisé	Lorsque vous activez le mode synchrone, un nœud de réplica est promu à l'état de nœud de réplica synchronisé. Le réplica synchronisé permet le basculement automatique du nœud principal.

Conditions préalables

- Configurez au moins deux nœuds de serveur autonomes. Pour plus d'informations, reportez-vous à la section [Configuration d'un serveur Orchestrator autonome](#).
- Synchronisez les horloges des machines virtuelles sur lesquelles les instances d'Orchestrator sont installées.
- Configurez un équilibrage de charge pour distribuer le trafic entre plusieurs instances d'Orchestrator.

Procédure

- 1 Connectez-vous à l'interface VAMI de l'environnement Orchestrator cible en tant que **root**.
Accédez à l'interface VAMI à l'adresse `https://IP_ou_nom_DNS_de_votre_serveur_orchestrator:5480`.
- 2 Sélectionnez l'onglet **Cluster** et entrez les informations d'identification du nœud Orchestrator qui sera le nœud principal du cluster.

Pour les environnements Orchestrator mis en cluster existants, entrez les informations d'identification du nœud principal du cluster Orchestrator.
- 3 Cliquez sur **Joindre un cluster**.
- 4 Passez en revue les informations du certificat du nœud et cliquez sur **OK**.
- 5 L'opération de clustering synchronise le contenu des nœuds Orchestrator et joint le nœud de réplica à la base de données PostgreSQL du nœud principal.

Étape suivante

Vérifiez que le cluster est configuré correctement sur la page **Valider la configuration** du centre de contrôle Orchestrator.

Note Suite à la configuration du nœud de cluster, le serveur Orchestrator redémarre automatiquement après 2 minutes. Une vérification de la configuration immédiatement après l'achèvement du processus peut renvoyer un état de cluster non valide.

Surveiller un cluster Orchestrator

Après avoir créé un cluster, vous pouvez surveiller les états des nœuds du cluster.

Vous pouvez surveiller les états de synchronisation de la configuration des instances d'Orchestrator ajoutées à un cluster à partir de la page **Gestion de cluster Orchestrator** du centre de contrôle.

État de synchronisation de la configuration	Description
EN COURS D'EXÉCUTION	Le service Orchestrator est disponible et peut accepter des demandes.
VEILLE	<p>Le service Orchestrator ne peut pas traiter les demandes parce que :</p> <ul style="list-style-type: none"> ■ 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 Orchestrator).
Impossible de récupérer l'état d'intégrité du service	Le service du serveur 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 Orchestrator redémarre automatiquement.

Activer le mode synchrone pour le cluster Orchestrator

Vous pouvez configurer un cluster de base de données Orchestrator pour qu'il s'exécute en mode synchrone.

Le mode synchrone permet le basculement automatique de la base de données Orchestrator principale. Le processus promeut l'un des nœuds de réplica à l'état de **réplica synchronisé**. Si le nœud principal actuel échoue, le réplica synchronisé est automatiquement promu à l'état de nœud principal. Le réplica synchronisé reçoit toutes les transactions terminées de la base de données du nœud principal.

Conditions préalables

Configurez un cluster Orchestrator composé d'au moins trois nœuds Orchestrator.

Procédure

- 1 Connectez-vous à l'interface VAMI de l'environnement Orchestrator cible en tant que **root**.

Accédez à l'interface VAMI à l'adresse `https://
IP_ou_nom_DNS_de_votre_serveur_orchestrator:5480`.

- 2 Sélectionnez l'onglet **Cluster**.
- 3 Cliquez sur **Mode synchrone**.
- 4 L'un des nœuds du cluster est promu à l'état de **réplica synchronisé**.

Pour confirmer la réussite de l'opération de synchronisation, vérifiez que l'état du mode de réplication dans l'onglet **Cluster** est **Base de données en mode synchrone**.

Promouvoir un nœud de réplica Orchestrator à l'état de nœud principal

Vous pouvez reconfigurer un cluster Orchestrator en promouvant un nœud de réplica à l'état de nœud principal.

Les nœuds Orchestrator peuvent être promus en mode asynchrone et synchrone.

Note Les clusters Orchestrator en mode synchrone disposent d'une fonction de basculement automatique. Par conséquent, si le nœud principal actuel échoue, le nœud de réplica synchronisé devient automatiquement le nouveau nœud principal.

Conditions préalables

Configurez un cluster Orchestrator composé d'au moins deux instances d'Orchestrator.

Procédure

- 1 Connectez-vous à l'interface VAMI de l'environnement Orchestrator cible en tant que **root**.
Accédez à l'interface VAMI à l'adresse `https://
IP_ou_nom_DNS_de_votre_serveur_orchestrator:5480`.
- 2 Sélectionnez l'onglet **Cluster**.
- 3 Cliquez sur **Promouvoir** en regard du nœud de réplica à promouvoir à l'état de nouveau nœud principal.
- 4 Le message **Promu à l'état de nouveau nœud master** s'affiche en haut à gauche de l'IU VAMI, et l'état du nœud est remplacé par **MASTER**.

Supprimer un nœud de cluster Orchestrator

Vous pouvez supprimer un nœud de réplica Orchestrator de votre cluster Orchestrator afin de pouvoir le remplacer ou d'en réduire la capacité.

Vous pouvez uniquement supprimer des nœuds de réplica du cluster. Pour supprimer un nœud principal, vous devez tout d'abord promouvoir un nœud de réplica pour le remplacer. Pour plus d'informations, reportez-vous à [Promouvoir un nœud de réplica Orchestrator à l'état de nœud principal](#).

Procédure

- 1 Connectez-vous à l'interface VAMI de l'environnement Orchestrator cible en tant que **root**.
Accédez à l'interface VAMI à l'adresse `https://
IP_ou_nom_DNS_de_votre_serveur_orchestrator:5480`.
- 2 Sélectionnez l'onglet **Cluster**.
- 3 Sélectionnez la commande **Supprimer** en regard du nœud de réplica.

- 4 Confirmez que vous souhaitez supprimer le nœud de réplica du cluster et cliquez sur **OK**.

Note Vous devez supprimer du serveur d'équilibrage de charge le nom d'hôte du nœud de réplica supprimé.

- 5 Le nœud Orchestrator est supprimé du cluster, et le message **Node was successfully deleted** s'affiche dans la partie supérieure gauche de l'interface utilisateur.

Configuration du programme d'amélioration du produit

Dans le cadre du programme d'amélioration du produit, VMware reçoit des informations anonymes dans le but de contribuer à améliorer la qualité, la fiabilité et la fonctionnalité des produits et 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 le programme d'amélioration du produit](#).

Rejoindre le programme d'amélioration du produit

Rejoignez le programme d'amélioration du produit à partir du centre de contrôle.

Procédure

- 1 Connectez-vous au centre de contrôle en tant qu'utilisateur **racine** et ouvrez la page **Programme d'amélioration du produit**.
- 2 Cochez la case **Rejoindre le programme d'amélioration du produit** pour activer le programme CEIP ou décochez la case pour désactiver le programme, puis cliquez sur **Enregistrer**.
- 3 (Facultatif) Décochez la case **Détection automatique de proxy** si vous souhaitez ajouter un hôte proxy manuellement.

Utilisation des services d'API

6

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

Le plug-in Configuration est inclus par défaut dans le module Orchestrator. Vous pouvez accéder aux workflows de configuration de plug-in à partir de la bibliothèque de workflows d'Orchestrator ou de l'API REST d'Orchestrator. Ces workflows vous permettent de modifier les paramètres du certificat approuvé et du keystore du serveur Orchestrator. Pour plus d'informations sur tous les appels de services disponibles de l'API REST d'Orchestrator, consultez la documentation *Référence de l'API REST Orchestrator*, disponible sur https://adresse_IP_ou_nom_DNS_du_serveur_orchestrator:8281/vco/api/docs.

- **Gestion des certificats SSL et des keystores à l'aide de l'API REST**

En plus de gérer des certificats SSL 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.

- **Automatisation de la configuration d'Orchestrator à l'aide de l'API REST du Centre de contrôle**

L'API REST du Centre de contrôle fournit un accès aux ressources pour la configuration du serveur Orchestrator. Vous pouvez utiliser l'API REST du Centre de contrôle avec des systèmes tiers pour automatiser la configuration d'Orchestrator.

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

En plus de gérer des certificats SSL 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 permettant d'importer et de supprimer des certificats SSL et des keystores. Vous pouvez accéder à ces workflows depuis **Bibliothèque > Configuration > Gestionnaire de confiance SSL et Keystores > de configuration > de la bibliothèque** dans la vue Workflows du client Orchestrator. Vous pouvez aussi exécuter ces workflows à l'aide de l'API REST d'Orchestrator.

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

Vous pouvez supprimer un certificat SSL en exécutant le workflow Supprimer un certificat approuvé 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 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 Fournissez 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 dans la demande.

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

Vous pouvez importer des certificats SSL 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. Pour plus d'informations sur l'importation de certificats dans Orchestrator à l'aide du Centre de contrôle, reportez-vous à [Gérer les certificats Orchestrator](#).

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 SSL. 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 SSL. Pour les services autres que HTTPS, le format pris en charge est <i>adresse_IP_ou_nom_DNS:port</i> . 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.

Automatisation de la configuration d'Orchestrator à l'aide de l'API REST du Centre de contrôle

L'API REST du Centre de contrôle fournit un accès aux ressources pour la configuration du serveur Orchestrator. Vous pouvez utiliser l'API REST du Centre de contrôle avec des systèmes tiers pour automatiser la configuration d'Orchestrator.

Le point de terminaison racine de l'API REST du Centre de contrôle est `https://{adresse_IP_ou_nom_DNS_du_serveur_orchestrator:8283}/vco-controlcenter/api`. Pour plus d'informations sur tous les appels de service disponibles que vous pouvez effectuer vers l'API REST du Centre de contrôle, consultez la documentation *Référence de l'API REST du Centre de contrôle*, sur `https://{adresse_IP_ou_nom_DNS_du_serveur_orchestrator:8283}/vco-controlcenter/docs`.

Utilitaire de ligne de commande

Vous pouvez utiliser l'utilitaire de ligne de commande d'Orchestrator pour automatiser la configuration d'Orchestrator.

Accédez à l'utilitaire de ligne de commande en vous connectant au dispositif Orchestrator Appliance en tant que racine sur SSH. L'utilitaire est situé dans `/var/lib/vco/tools/configuration-cli/bin`. Pour afficher les options de configuration disponibles, exécutez `./vro-configure.sh --help`.

Options de configuration supplémentaires

7

Vous pouvez modifier le comportement par défaut d'Orchestrator à l'aide du Centre de contrôle.

Ce chapitre contient les rubriques suivantes :

- [Reconfiguration de l'authentification](#)
- [Exporter la configuration Orchestrator](#)
- [Importer la configuration d'Orchestrator](#)
- [Configuration des propriétés d'exécution de workflow](#)
- [Fichiers journaux d'Orchestrator](#)
- [Ajouter des cartes réseau](#)
- [Configurer des itinéraires statiques](#)

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.

Conditions préalables

Procédure

- 1 Connectez-vous au centre de contrôle en tant que **root**.
- 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.

- 3 Dans la section **SERVICE D'IDENTITÉ**, cliquez sur **DÉSINSCRIRE** pour supprimer les informations d'identification du serveur.

Résultats

Vous avez désinscrit le fournisseur d'authentification.

Étape suivante

Reconfigurez l'authentification dans le centre de contrôle. Pour plus d'informations, reportez-vous à la section [Configurer un serveur Orchestrator autonome avec l'authentification vRealize Automation](#) ou [Configurer un serveur Orchestrator autonome avec l'authentification vSphere](#).

Modifier les paramètres d'authentification

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

Conditions préalables

- Connectez-vous au centre de contrôle en tant que **root**.
- Sélectionnez le mode d'authentification et configurez les paramètres de connexion du fournisseur d'authentification.

Procédure

- 1 Modifiez le locataire par défaut.

Note Pour pouvoir modifier le locataire par défaut, il faut utiliser le mode d'authentification vRealize Automation.

- a Sur la page **Configurer le fournisseur d'authentification** du centre de contrôle, cliquez sur le bouton **MODIFIER** en regard de la zone de texte **Locataire par défaut**.
- b Dans la zone de texte, renommez le locataire par défaut existant.
- c 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.

- d Entrez le nom d'un groupe d'administrateurs et cliquez sur **RECHERCHER**.
- e Dans la liste des groupes, double-cliquez sur le nom du groupe pour le sélectionner.
- f Cliquez sur **ENREGISTRER LES MODIFICATIONS**.

Vous êtes déconnecté du centre de contrôle et redirigé vers l'écran de connexion Single Sign-On.

2 Modifiez le groupe d'administrateurs.

- a Cliquez sur le bouton **MODIFIER** en regard de la zone de texte **Groupe admin**.
- b Entrez le nom d'un groupe d'administrateurs et cliquez sur **RECHERCHER**.
- c Dans la liste des groupes, double-cliquez sur le nom du groupe pour le sélectionner.
- d Cliquez sur **ENREGISTRER LES MODIFICATIONS**.

Vous êtes déconnecté du centre de contrôle et redirigé vers l'écran de connexion Single Sign-On.

Exporter la configuration Orchestrator

Le Centre de contrôle propose un mécanisme pour exporter les paramètres de configuration d'Orchestrator dans un fichier local. Vous pouvez utiliser ce mécanisme pour capturer à tout moment un snapshot de votre configuration système et importer cette configuration dans une nouvelle instance d'Orchestrator.

Vous devez exporter et enregistrer régulièrement vos paramètres de configuration, notamment après des modifications, des tâches de maintenance ou des mises à niveau du système.

Important Conservez le fichier contenant la configuration exportée en lieu sûr car il contient des informations administratives sensibles.

Procédure

- 1 Connectez-vous au centre de contrôle en tant que **root**.
- 2 Cliquez sur **Exporter/importer la configuration**.
- 3 Sélectionnez le type de fichier que vous voulez exporter.

Note Si vous sélectionnez **Exporter les configurations de plug-in** et que les configurations de plug-in contiennent des propriétés chiffrées, vous devez également sélectionner **Exporter la configuration du serveur** pour réussir à déchiffrer les données lors de l'importation.

- 4 (Facultatif) Saisissez un mot de passe pour protéger le fichier de configuration.
Utilisez le même mot de passe lorsque vous importerez la configuration ultérieurement.
- 5 Cliquez sur **Exporter**.

Résultats

Orchestrator crée un fichier `orchestrator-config-export-hostname-dateReference.zip` qui est téléchargé sur votre machine locale. Vous pouvez utiliser ce fichier pour cloner ou restaurer le système.

Importer la configuration d'Orchestrator

Vous avez la possibilité de restaurer une configuration système précédemment exportée après une réinstallation d'Orchestrator ou une défaillance du système.

Si vous employez la procédure d'importation pour cloner la configuration d'Orchestrator, la configuration du plug-in vCenter Server n'est plus valide et ne fonctionne plus car un nouvel ID est généré pour le plug-in vCenter Server.

Procédure

- 1 Connectez-vous au centre de contrôle en tant que **root**.
- 2 Cliquez sur **Exporter/Importer la configuration** et accédez à l'onglet **Importer la configuration**.
- 3 Localisez et sélectionnez le fichier .zip que vous avez exporté de votre précédente installation.

Note La syntaxe par défaut du fichier de configuration exporté est `orchestrator-config-export-hostname-dateofexport_timeofexport.zip`

- 4 (Facultatif) Saisissez le mot de passe utilisé pour exporter la configuration.

Cette étape n'est pas nécessaire si vous n'avez pas exporté la configuration en utilisant un mot de passe.

- 5 Sélectionner le type d'importation :

Option	Description
Intégrée	Migrates vers une instance d'Orchestrator intégrée à vRealize Automation.
Externe	Migre vers un serveur Orchestrator externe.
Réplica	Réplique la même instance d'Orchestrator.

- 6 Cliquez sur **Importer**.

Résultats

Le nouveau système réplique l'ancienne configuration, en fonction du type d'importation sélectionné. Le service du serveur Orchestrator redémarre automatiquement.

Étape suivante

Vérifiez qu'Orchestrator est configuré correctement sur la page **Valider la configuration** dans le Centre de contrôle.

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 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.

Sur la page **Options avancées** du centre de contrôle, vous pouvez configurer les propriétés d'exécution de workflow.

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 Orchestrator.
Nombre de workflows en cours d'exécution simultanée	Nombre maximal de workflows de nœud Orchestrator simultanés exécutés en même temps.
Quantité maximale de workflows en cours d'exécution dans la file d'attente	Nombre de demandes d'exécution de workflow accepté par le nœud Orchestrator avant son indisponibilité.
Nombre maximal d'exécutions conservées par workflow	Nombre maximal d'exécutions de workflows terminées conservées en historique par workflow dans un cluster. Dès que le nombre est dépassé, l'exécution la plus ancienne est supprimée.
Jours d'expiration des événements du journal	Nombre de jours durant lesquels les événements du journal pour un cluster sont conservés dans la base de données avant la purge.
Décrire toutes les exécutions de workflows	Activez et désactivez le profilage automatique de workflow. Lorsqu'il est activé, le profilage de workflow génère des données de mesure sur chaque exécution de workflow.
Intervalle de distribution des statistiques du profileur de workflows	Intervalle pendant lequel les statistiques du profileur seront distribuées sur chaque instance d'Orchestrator dans votre environnement.

Fichiers journaux d'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.

Vous pouvez télécharger un bundle compressé qui inclut les fichiers de configuration et les fichiers journaux d'Orchestrator à partir du menu **Exporter les journaux** dans le Centre de contrôle.

Tableau 7-1. Liste des fichiers journaux d'Orchestrator

Nom du fichier	Emplacement	Description
scripting.log	/var/log/vco/app-server	Fournit des messages du journal de scripts des workflows et des actions. Utilisez le fichier scripting.log pour isoler les workflows et actions exécutés à partir des opérations normales d'Orchestrator. Ces informations sont également incluses dans le fichier server.log.
server.log	/var/log/vco/app-server	Fournit des informations sur toutes les activités concernant le serveur Orchestrator. Analysez le fichier server.log lorsque vous déboguez Orchestrator ou toute application qui s'exécute sur Orchestrator.
metrics.log	/var/log/vco/app-server	Contient des informations d'exécution concernant le serveur. Les informations sont ajoutées à ce fichier journal toutes les 5 minutes.
localhost_access_log.txt	/var/log/vco/app-server	Il s'agit du journal des requêtes HTTP du serveur.
localhost_access_log.date.txt	/var/log/vco/configuration	Il s'agit du journal des requêtes HTTP du service du Centre de contrôle.
controlcenter.log	/var/log/vco/configuration	Le fichier journal du service du Centre de contrôle.

Permanence des consignations

Vous pouvez consigner des informations de journaux dans n'importe quel type de script Orchestrator, tel que les workflows, stratégies ou actions. Ces informations sont de différents types et niveaux. Le type peut être permanent ou non permanent. Le niveau peut être DEBUG, INFO, WARN, ERROR, TRACE et FATAL.

Tableau 7-2. Création de journaux permanents et non permanents

Niveau de consignation	Type permanent	Type non permanent
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.error("texte");

Journaux permanents

Les journaux permanents (journaux du serveur) effectuent un suivi des journaux d'exécution des workflows et sont stockés dans la base de données Orchestrator. Pour afficher les journaux du serveur, vous devez sélectionner un workflow, une exécution de workflow terminée ou une stratégie et cliquer sur l'onglet **Événements** dans le client Orchestrator.

Journaux non permanents

Lorsque vous créez des scripts à l'aide d'un journal non permanent (journal système), le serveur Orchestrator notifie la présence de ce journal à toutes les applications Orchestrator en cours d'exécution, mais ces informations ne sont pas stockées dans la base de données. Les informations du journal sont perdues lorsque l'application est redémarrée. Les journaux non permanents sont utilisés à des fins de débogage et pour obtenir des informations en direct. Pour afficher les journaux système, vous devez sélectionner une exécution de workflow terminée dans le client Orchestrator et cliquer sur **Journaux** dans l'onglet **Schéma**.

Configuration des journaux d'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.

Paramètres de rotation des journaux

Pour éviter que la taille du journal de serveur ne devienne trop conséquente, vous pouvez définir la taille et le nombre maximal du fichier du journal de serveur en modifiant les valeurs des zones de texte **Nombre de fichiers max** et **Taille de fichier max (Mo)**.

Exportation de fichiers journaux d'Orchestrator

Sur la page **Exporter les journaux** du centre de contrôle, vous pouvez générer une archive ZIP des informations de dépannage contenant les fichiers journaux d'installation, de configuration, de serveur et de wrapper.

Les informations du journal sont stockées dans une archive ZIP nommée `vco-logs-date_hour.zip`.

Note Lorsqu'un cluster comprend plusieurs instances Orchestrator, l'archive ZIP inclut les journaux de toutes ces instances.

Filtrer les journaux d'Orchestrator

Vous pouvez filtrer les journaux du serveur Orchestrator en fonction d'une exécution de workflow spécifique et collecter les données de diagnostic de cette exécution.

Les journaux d'Orchestrator contiennent de nombreuses informations utiles que vous pouvez surveiller en temps réel. Lorsque plusieurs instances du même workflow s'exécutent en même temps, vous pouvez filtrer les données de diagnostic de chaque exécution dans le flux de journal en direct d'Orchestrator, de manière à suivre les différentes exécutions.

Note Lorsqu'un cluster contient plusieurs instances Orchestrator, le flux de journal en direct affiche uniquement les journaux du nœud Orchestrator local.

Procédure

- 1 Connectez-vous au centre de contrôle en tant que **root**.
- 2 Cliquez sur **Flux de journal en direct**.
- 3 Dans la barre de recherche, entrez vos paramètres de recherche.

Par exemple, vous pouvez filtrer les journaux par nom d'utilisateur, nom du workflow, ID de workflow ou ID de jeton.
- 4 (Facultatif) Sélectionnez **Sensible à la casse** et **Filtre (grep)** pour filtrer davantage les résultats de la recherche.

Si vous sélectionnez **Filtre (grep)**, le flux en direct affiche uniquement les lignes qui correspondent à vos paramètres de recherche.

Résultats

Le flux de journal en direct d'Orchestrator est filtré en fonction de vos paramètres de recherche.

Étape suivante

Pour filtrer d'anciens journaux non accessibles via la page **Flux de journal en direct** du centre de contrôle, vous pouvez utiliser des outils d'analyse des journaux tiers.

Configuration de l'intégration de la journalisation avec le serveur distant

Vous pouvez configurer Orchestrator pour qu'il envoie des journaux à des systèmes de journalisation distants tels que vRealize Log Insight ou d'autres serveurs Syslog.

Procédure

- 1 Connectez-vous au centre de contrôle en tant que **root**.
- 2 Accédez au menu **Intégration de la journalisation**.
- 3 Ouvrez **Activer la journalisation pour un serveur de journal distant**.

- 4 Configurez les options d'intégration de la journalisation.
 - a Sélectionnez le type de système de journalisation.
 - b Entrez le nom d'hôte et la valeur de port du serveur de journalisation distant.
 - c Sélectionnez le protocole utilisé pour envoyer des événements de journaux au serveur de journalisation distant.
- 5 Pour terminer la configuration de l'intégration de la journalisation sur le serveur distant, cliquez sur **Enregistrer**.

Ajouter des cartes réseau

vRealize Orchestrator prend en charge plusieurs cartes réseau. Après l'installation, vous pouvez ajouter des cartes réseau à Orchestrator Appliance.

Conditions préalables

Installez complètement vRealize Orchestrator dans votre environnement vCenter Server.

Procédure

- 1 Dans vCenter Server, ajoutez des cartes réseau à chaque dispositif vRealize Orchestrator Appliance.
 - a Cliquez avec le bouton droit sur le dispositif et sélectionnez **Modifier les paramètres**.
 - b Ajoutez des cartes réseau VMXNET3.
 - c S'il est sous tension, redémarrez le dispositif.
- 2 Connectez-vous à l'interface de gestion du dispositif vRealize Orchestrator Appliance en tant qu'utilisateur racine.
https://adresse_ip_orchestrator_appliance:5480
- 3 Sélectionnez **Réseau**, puis vérifiez que plusieurs cartes réseau sont disponibles.
- 4 Sélectionnez **Adresse** et configurez l'adresse IP des cartes réseau.

Tableau 7-3. Exemple de configuration de carte réseau

Configuration	Valeur
Type d'adresse IPv4	Statique
Adresse IPv4	172.22.0.2
Masque de réseau	255.255.255.0

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

Configurer des itinéraires statiques

Lors de l'ajout de cartes réseau à une installation vRealize Orchestrator, si vous avez besoin d'itinéraires statiques, ouvrez une session d'invite de commandes pour les configurer.

Conditions préalables

Ajoutez plusieurs cartes réseau pour les dispositifs vRealize Orchestrator Appliance.

Procédure

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

- 2 Ouvrez le fichier d'itinéraires dans un éditeur de texte.

```
/etc/sysconfig/network/routes
```

- 3 Recherchez la ligne `default` pour la passerelle par défaut, mais ne la modifiez pas.

Note Si vous devez changer la passerelle par défaut, utilisez plutôt l'interface de gestion de vRealize Orchestrator.

- 4 Sous la ligne `default`, ajoutez de nouvelles lignes pour les itinéraires statiques. Par exemple :

```
default 10.10.10.1 - -  
172.30.30.0 192.168.100.1 255.255.255.0 eth0  
192.168.210.0 192.168.230.1 255.255.255.0 eth2
```

- 5 Enregistrez et fermez le fichier d'itinéraires.
- 6 Redémarrez le dispositif.
- 7 Dans les clusters HA, répétez le processus pour chaque dispositif.

Cas d'utilisation de configuration et dépannage

8

Vous pouvez configurer le serveur Orchestrator pour qu'il fonctionne avec le dispositif vCenter Server, et également désinstaller les plug-ins Orchestrator ou modifier les certificats autosignés.

Les cas d'utilisation de configuration fournissent des flux de tâches que vous pouvez effectuer pour répondre aux exigences de configuration spécifiques de votre serveur Orchestrator, ainsi que des rubriques de dépannage pour comprendre et résoudre un problème, s'il existe une solution.

Ce chapitre contient les rubriques suivantes :

- [Configurer le plug-in vRealize Orchestrator pour vSphere Web Client](#)
- [Annuler l'enregistrement de l'authentification Orchestrator](#)
- [Modification des certificats SSL](#)
- [Annuler des workflows en cours d'exécution](#)
- [Permettre le débogage du serveur Orchestrator](#)
- [Sauvegarder les éléments et la configuration de Orchestrator](#)
- [Sauvegarde et restauration de vRealize Orchestrator](#)
- [Récupération d'urgence d'Orchestrator à l'aide de Site Recovery Manager](#)

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 du système 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

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.

Procédure

- 1 Connectez-vous au client vRealize Orchestrator.
- 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 (Facultatif) Entrez `https://votre_nom_d'hôte_orchestrator:8281` ou l'URL de service de l'équilibreur de charge qui redirige les demandes vers les nœuds de serveur vRealize Orchestrator.
- 6 Cliquez sur **Exécuter**.

Annuler l'enregistrement de l'authentification Orchestrator

Annulez l'enregistrement d'Orchestrator en tant que solution Single Sign-On à partir de la page Configurer le fournisseur d'authentification du Centre de contrôle.

Si vous souhaitez reconfigurer l'authentification Orchestrator vCenter Single Sign-On ou vRealize Automation, vous devez d'abord annuler l'enregistrement de l'authentification Orchestrator.

Procédure

- 1 Connectez-vous au centre de contrôle en tant que **root**.
- 2 Cliquez sur **Configurer le fournisseur d'authentification**.
- 3 Cliquez sur **Annuler l'enregistrement**.
- 4 (Facultatif) Si vous souhaitez supprimer des données d'inscription du serveur d'identité, entrez vos informations d'identification.
- 5 Cliquez sur **Annuler l'enregistrement** à partir de la section **Service d'identité**.

Résultats

Vous avez annulé l'enregistrement de votre instance de serveur Orchestrator.

Modification des certificats SSL

Par défaut, le serveur Orchestrator utilise un certificat SSL autosigné pour communiquer à distance avec le client Orchestrator. Vous pouvez remplacer les certificats SSL si, par exemple, la stratégie de sécurité de votre société nécessite que vous utilisiez ses certificats SSL.

Lorsque vous tentez d'utiliser Orchestrator via une connexion Internet SSL sécurisée et que vous ouvrez le Centre de contrôle dans un navigateur Web, vous recevez un avertissement indiquant que la connexion n'est pas fiable, si vous utilisez Mozilla Firefox, ou que le certificat de sécurité du site Web présente des problèmes, si vous utilisez Internet Explorer.

Après avoir cliqué sur **Continuer sur ce site Web (non recommandé)**, même si vous avez importé le certificat SSL dans le magasin de certificats de confiance, la notification Erreur de certificat s'affichera toujours en rouge dans la barre d'adresse du navigateur Web. Vous pouvez travailler avec Orchestrator dans le navigateur Web, mais il est possible qu'un système tiers ne fonctionne pas correctement lorsque vous tentez d'accéder à l'API via HTTPS.

Vous pouvez également recevoir un avertissement de certificat lorsque vous démarrez le client Orchestrator et tentez de vous connecter au serveur Orchestrator via une connexion SSL.

Vous pouvez résoudre le problème en installant un certificat signé par une autorité de certification commerciale (CA). Pour arrêter de recevoir un avertissement de certificat de la part du client Orchestrator, ajoutez votre certificat d'autorité de certification racine au keystore Orchestrator sur la machine sur laquelle le client Orchestrator est installé.

Ajout d'un certificat au magasin local

Après avoir reçu un certificat d'une autorité de certification, vous devez ajouter le certificat à votre stockage local pour qu'il fonctionne avec le Centre de contrôle sans recevoir d'avertissements de certificat ou de messages d'erreur.

Ce workflow décrit le processus d'ajout du certificat à votre stockage local à l'aide d'Internet Explorer.

- 1 Ouvrez Internet Explorer et accédez à `https://adresse_IP_ou_nom_DNS_du_serveur_orchestrator:8283/`.
- 2 Lorsque vous y êtes invité, cliquez sur **Continuer vers ce site Web (non recommandé)**.
L'erreur de certificat apparaît à droite de la barre d'adresse dans Internet Explorer.
- 3 Cliquez sur l'erreur de certificat et sélectionnez **Afficher les certificats**.
- 4 Cliquez sur **Installer les certificats**.
- 5 Sur la page d'accueil de l'**Assistant d'importation de certificat**, cliquez sur **Suivant**.
- 6 Dans la fenêtre du **magasin de certificats**, sélectionnez **Placer tous les certificats dans le magasin suivant**.
- 7 Recherchez et sélectionnez **Autorité de certification racine approuvée**.
- 8 Terminez l'assistant et redémarrez Internet Explorer.

9 Accédez au serveur Orchestrator via votre connexion SSL.

Vous ne recevez plus d'avertissements et aucune erreur de certificat ne s'affiche dans la barre d'adresse.

D'autres applications et systèmes, tels que VMware Service Manager, doivent avoir accès aux API REST d'Orchestrator via une connexion SSL.

Modifier le certificat du site de gestion du dispositif Orchestrator Appliance

Le dispositif Orchestrator Appliance utilise `lighttpd` pour exécuter son propre site de gestion. Vous pouvez remplacer le certificat SSL du site de gestion Orchestrator Appliance, par exemple, si la stratégie de sécurité de votre société nécessite que vous utilisiez ses certificats SSL.

Conditions préalables

Par défaut, le certificat SSL du dispositif Orchestrator Appliance et la clé privée sont stockés dans un fichier PEM situé à l'emplacement `/opt/vmware/etc/lighttpd/server.pem`. Pour installer un nouveau certificat, assurez-vous d'exporter votre nouveau certificat SSL et la clé privée du keystore Java vers un fichier PEM.

Procédure

- 1 Connectez-vous à la console Linux du dispositif Orchestrator Appliance en tant que racine.
- 2 Localisez le fichier `/opt/vmware/etc/lighttpd/lighttpd.conf` et ouvrez-le dans un éditeur.
- 3 Recherchez la ligne suivante :

```
#### SSL engine
ssl.engine = "enable"
ssl.pemfile = "/opt/vmware/etc/lighttpd/server.pem"
```

- 4 Modifiez l'attribut `ssl.pemfile` afin qu'il pointe vers le fichier PEM contenant votre nouveau certificat SSL et la clé privée.
- 5 Enregistrez le fichier `lighttpd.conf`.
- 6 Pour redémarrer le serveur `lighttpd`, exécutez la commande suivante :

```
service vami-lighttp restart
```

Résultats

Vous avez modifié le certificat du site de gestion du dispositif Orchestrator Appliance.

Annuler des workflows en cours d'exécution

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

Procédure

- 1 Connectez-vous au centre de contrôle en tant que **root**.
- 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.

Étape suivante

Vérifiez que les workflows sont annulés sur la page **Inspecter les workflows** du Centre de contrôle.

Permettre le débogage du serveur Orchestrator

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

Procédure

- 1 Connectez-vous au centre de contrôle en tant que **root**.
- 2 Cliquez sur **Débogage d'Orchestrator**.
- 3 Cliquez sur **Activer le débogage**.
- 4 (Facultatif) Entrez un port différent de celui par défaut.
- 5 (Facultatif) Cliquez sur **Interrompre**.

En sélectionnant cette option, vous devez attacher un débogueur avant de lancer le serveur Orchestrator.

- 6 Cliquez sur **Enregistrer**.
- 7 Ouvrez la page Options de démarrage dans le Centre de contrôle et cliquez sur **Redémarrez**.

Résultats

Le serveur Orchestrator est interrompu au démarrage jusqu'à ce que vous attachiez un débogueur Java distant au port défini.

Sauvegarder les éléments et la configuration de Orchestrator

Sauvegardez votre configuration du serveur Orchestrator personnalisée et vos éléments de workflow, pour vous assurer qu'ils pourront être réutilisés par les autres instances d'Orchestrator.

Si vous modifiez des actions, des stratégies, des éléments de configuration ou des workflows standard, et si vous importez ensuite un module contenant les mêmes éléments avec un numéro de version Orchestrator ultérieur, les modifications apportées aux éléments sont perdues. Vous pouvez éviter de perdre des workflows personnalisés et d'autres éléments en les exportant avant de migrer votre instance d'Orchestrator.

Chaque instance de serveur Orchestrator présente des certificats uniques, et chaque instance de plug-in vCenter Server dispose d'un ID unique. Ces certificats et cet ID unique définissent l'identité du serveur Orchestrator et du plug-in vCenter Server. Si vous ne sauvegardez pas les éléments Orchestrator ou si vous n'exportez pas la configuration de Orchestrator à des fins de sauvegarde, assurez-vous de modifier ces identifiants.

Conditions préalables

Déployez et configurez une nouvelle instance de serveur Orchestrator. Reportez-vous à la section [Configuration d'un serveur Orchestrator autonome](#).

Procédure

- 1 Exportez la configuration Orchestrator.
 - a Connectez-vous au centre de contrôle en tant que **root**.
 - b Cliquez sur **Exporter/importer la configuration**.
 - c Sélectionnez les types de fichier que vous voulez exporter.
 - d (Facultatif) Protégez le fichier de configuration en saisissant un mot de passe.
Utilisez le même mot de passe lorsque vous importez la configuration.
 - e Cliquez sur **Exporter**.
- 2 Connectez-vous à l'application du client Orchestrator.
- 3 Créez un module contenant tous les éléments Orchestrator que vous avez créés ou modifiés.
 - a Sous la vue **Administrer**, cliquez sur l'onglet **Modules**.
 - b Cliquez sur le bouton de menu dans la barre de titre de la liste des modules, puis sélectionnez **Ajouter un module**.

- c Entrez un nom pour le nouveau module et cliquez sur **OK**.

La syntaxe des noms de modules est *domain.votre_société.dossier.nom_du_module*.

Par exemple, `com.vmware.myfolder.mypackage`.

- d Cliquez avec le bouton droit sur le module, puis sélectionnez **Modifier**.
- e Dans l'onglet **Général** ajoutez une description du module.
- f Dans l'onglet **Workflows**, ajoutez des workflows au module.
- g (Facultatif) Ajoutez des modèles de stratégie, des actions, des éléments de configuration et de ressource, des droits d'accès et des plug-ins au module.
- h Cliquez sur **Enregistrer et fermer**.

4 Exportez le module.

- a Cliquez avec le bouton droit sur le module que vous souhaitez exporter et sélectionnez **Exporter un module**.
- b Recherchez et sélectionnez l'emplacement où vous souhaitez enregistrer le module.
- c (Facultatif) Utilisez le certificat correspondant pour signer le module.
- d (Facultatif) Imposez des restrictions sur le module exporté.
- e (Facultatif) Pour appliquer des restrictions au contenu du module exporté, désélectionnez les options, selon les besoins.

Option	Description
Exporter l'historique des versions	L'historique des versions du module n'est pas exporté.
Exporter les valeurs des paramètres de configuration	Les valeurs d'attribut des éléments de configuration du module ne sont pas exportées.
Exporter des balises globales	Les balises globales du module ne sont pas exportées.

Note L'option **Exporter les valeurs des paramètres de configuration SecureString** est désélectionnée par défaut. L'exportation de ces paramètres de configuration peut entraîner un problème de sécurité. Soyez prudent lorsque vous l'utilisez.

- f Cliquez sur **Enregistrer**.

5 Importez la configuration Orchestrator exportée au préalable dans la nouvelle instance du serveur Orchestrator.

- a Connectez-vous au centre de contrôle dans la nouvelle instance d'Orchestrator en tant que **root**.
- b Cliquez sur **Exporter/Importer la configuration** et accédez à l'onglet **Importer la configuration**.
- c Recherchez et sélectionnez le fichier .zip que vous avez exporté lors de votre installation précédente.

- d Tapez le mot de passe que vous avez utilisé lors de l'exportation de la configuration.
Cette étape n'est pas nécessaire si vous n'avez pas défini de mot de passe.
- e Sélectionnez le type d'importation.
- f Cliquez sur **Importer**.

6 Importez le module que vous avez exporté dans la nouvelle instance d'Orchestrator.

- a Connectez-vous à l'application du client Orchestrator de la nouvelle instance d'Orchestrator.
- b Dans le menu déroulant du client Orchestrator, sélectionnez **Administrer**.
- c Cliquez sur l'onglet **Modules**.
- d Cliquez sur le bouton de menu dans la barre de titre de la liste des modules, puis sélectionnez **Importer un module**.
- e Recherchez et sélectionnez le module que vous souhaitez importer, puis cliquez sur **Ouvrir**.

Les informations de certificat de l'exportateur s'affichent.

- f Vérifiez les détails d'importation du module et sélectionnez **Importer** ou **Importer et faire confiance au fournisseur**.

La vue Importer un module apparaît. Si la version de l'élément du module importé est plus récente que la version du serveur, le système sélectionne l'élément à importer automatiquement.

- g Sélectionnez les éléments que vous souhaitez importer.

Note Sélectionnez les éléments personnalisés pour lesquels des versions ultérieures existent.

- h (Facultatif) Décochez la case **Importer les valeurs des paramètres de configuration** si vous ne désirez pas importer les valeurs d'attributs des éléments de configuration issus du module.
- i Dans le menu déroulant, indiquez si vous souhaitez importer les balises provenant du module.

Option	Description
Importer les balises, mais conserver les valeurs existantes	Importez les balises provenant du module sans remplacer les valeurs des balises existantes.
Importer des balises et remplacer les valeurs existantes	Importez les balises provenant du module et remplacez leurs valeurs.
Ne pas importer les balises	N'importez pas les balises du module.

- j Cliquez sur **Importer les éléments sélectionnés**.

Résultats

Vous avez bien sauvegardé la configuration d'Orchestrator et les éléments.

Sauvegarde et restauration de vRealize Orchestrator

Vous pouvez utiliser vSphere Data Protection pour sauvegarder et restaurer une machine virtuelle (VM) contenant une instance vRealize Orchestrator.

vSphere Data Protection est une solution de sauvegarde et de récupération sur disque VMware conçue pour les environnements vSphere. vSphere Data Protection est entièrement intégrée à vCenter Server. vSphere Data Protection vous permet de gérer les tâches de sauvegarde et de stocker les sauvegardes dans des emplacements de stockage dédupliqués. Après le déploiement et la configuration de vSphere Data Protection, vous pouvez accéder à vSphere Data Protection à l'aide de l'interface vSphere Web Client pour sélectionner, planifier, configurer et gérer les sauvegardes et les récupérations de machines virtuelles. Lors d'une sauvegarde, vSphere Data Protection crée un snapshot mis au repos de la machine virtuelle. Une déduplication est automatiquement réalisée lors de chaque opération de sauvegarde.

Pour plus d'informations sur le déploiement et la configuration de vSphere Data Protection, consultez la documentation de *vSphere Data Protection Administration*.

Sauvegarder vRealize Orchestrator

Vous pouvez sauvegarder votre instance de vRealize Orchestrator en tant que machine virtuelle.

Pour vous assurer que tous les composants d'une VM dans un seul produit sont sauvegardés ensemble, stockez les VM de votre environnement vRealize Orchestrator dans un seul dossier vCenter Server et créez une tâche de stratégie de sauvegarde pour ce dossier.

Conditions préalables

- Vérifiez que le dispositif vSphere Data Protection est déployé et configuré. Pour plus d'informations sur le déploiement et la configuration de vSphere Data Protection, consultez la documentation *vSphere Data Protection Administration*.
- Utilisez vSphere Web Client pour vous connecter à l'instance de vCenter Server qui gère votre environnement. Connectez-vous en tant qu'utilisateur avec les privilèges d'administrateur utilisés lors de la configuration de vSphere Data Protection.

Procédure

- 1 Sur la page d'accueil de vSphere Web Client, cliquez sur **vSphere Data Protection**.
- 2 Sélectionnez votre dispositif vSphere Data Protection dans le menu déroulant du **dispositif VDP** et cliquez sur **Se connecter**.
- 3 Dans l'onglet **Mise en route**, cliquez sur **Créer une tâche de sauvegarde**.
- 4 Cliquez sur **Images invitées** pour sauvegarder votre instance de vRealize Orchestrator, puis sur **Suivant**.

- 5 Sélectionnez **Image complète** pour sauvegarder l'intégralité de la machine virtuelle et cliquez sur **Suivant**.
- 6 Développez l'arborescence **Machines virtuelles** et cochez la case correspondant à votre VM vRealize Orchestrator.
- 7 Suivez les invites afin de définir la planification de sauvegarde, la stratégie de conservation et le nom de la tâche de sauvegarde.

Pour plus d'informations sur la sauvegarde et la restauration des machines virtuelles, reportez-vous à la documentation *vSphere Data Protection Administration*.

Votre tâche de sauvegarde s'affiche dans la liste des tâches de sauvegarde sous l'onglet **Sauvegarde**.
- 8 (Facultatif) Ouvrez l'onglet **Sauvegarde**, sélectionnez la tâche de sauvegarde et cliquez sur **Sauvegarder maintenant** pour sauvegarder votre vRealize Orchestrator.

Note Vous pouvez également attendre le démarrage automatique de la sauvegarde selon la planification que vous avez définie.

Le processus de sauvegarde s'affiche dans la page **Tâches récentes**.

Résultats

L'image de votre VM s'affiche dans la liste des sauvegardes sous l'onglet **Restaurer**.

Étape suivante

Ouvrez l'onglet **Restaurer** et vérifiez que l'image de votre VM se trouve dans la liste des sauvegardes.

Restaurer une instance de vRealize Orchestrator

Vous pouvez restaurer votre instance de vRealize Orchestrator à son emplacement d'origine ou à un emplacement différent sur le même dispositif vCenter Server.

Conditions préalables

- Vérifiez que le dispositif vSphere Data Protection est déployé et configuré. Pour plus d'informations sur le déploiement et la configuration de vSphere Data Protection, consultez la documentation *vSphere Data Protection Administration*.
- Sauvegardez votre instance de vRealize Orchestrator. Reportez-vous à la section [Sauvegarder vRealize Orchestrator](#).
- Utilisez vSphere Web Client pour vous connecter à l'instance de vCenter Server qui gère votre environnement. Connectez-vous en tant qu'utilisateur avec les privilèges d'administrateur utilisés lors de la configuration de vSphere Data Protection.

Procédure

- 1 Sur la page d'accueil de vSphere Web Client, cliquez sur **vSphere Data Protection**.

- 2 Sélectionnez votre dispositif vSphere Data Protection dans le menu déroulant du **dispositif VDP** et cliquez sur **Connecter**.
- 3 Ouvrez l'onglet **Restaurer**.
- 4 Dans la liste des tâches de sauvegarde, sélectionnez la sauvegarde vRealize Orchestrator à restaurer.

Note Si vous disposez de plusieurs VM, vous devez les restaurer simultanément pour les synchroniser.

- 5 Pour restaurer votre instance de vRealize Orchestrator sur le même dispositif vCenter Server, cliquez sur l'icône **Restaurer** et suivez les invites pour définir l'emplacement de restauration de vRealize Orchestrator sur votre dispositif vCenter Server.

Ne sélectionnez pas **Mettre sous tension**, car le dispositif doit être le dernier composant à être mis sous tension. Pour plus d'informations sur la sauvegarde et la restauration d'une machine virtuelle, reportez-vous à la documentation *vSphere Data Protection Administration*.

Un message s'affiche et indique que la restauration a été lancée.

- 6 (Facultatif) Mettez vos hôtes de base de données sous tension s'ils sont externes et restaurez la configuration de votre équilibrage de charge.
- 7 Mettez sous tension le dispositif vRealize Orchestrator Appliance.

Résultats

La VM vRealize Orchestrator restaurée s'affiche dans l'inventaire de vCenter Server.

Étape suivante

Vérifiez que vRealize Orchestrator est correctement configuré en ouvrant la page **Valider la configuration** dans le Centre de contrôle.

Récupération d'urgence d'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 5.5 est installé sur les sites protégés et de récupération.
- Vérifiez que vous utilisez Site Recovery Manager 5.8.
- 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 les machines virtuelles.

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
- Configurer vSphere Replication sur les machines virtuelles
- Effectuer certaines ou toutes les actions ci-dessus

Procédure

- 1 Dans vSphere Web Client, sélectionnez **Récupération de site > Groupes de protection**.
- 2 Sous l'onglet **Objets**, cliquez sur l'icône pour créer un groupe de protection.
- 3 Sur la page Type de groupe de protection, sélectionnez le site protégé, puis le type de réplication et cliquez sur **Suivant**.

Option	Action
Groupes de réplication basée sur la baie	Sélectionnez Réplication basée sur les baies (ABR) et sélectionnez une paire de baies.
Groupe de protection vSphere Replication	Sélectionnez vSphere Replication .

- 4 Sélectionnez des groupes de banque de données ou des machines virtuelles 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 .
Groupes de protection vSphere Replication	Sélectionnez des machines virtuelles dans la liste, puis cliquez sur Suivant .

Lorsque vous créez des groupes de protection vSphere Replication, seules les machines virtuelles que vous avez configurées pour vSphere Replication et qui ne sont pas déjà dans un groupe de protection apparaissent dans la liste.

- 5 Passez en revue vos paramètres et cliquez sur **Terminer**.

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

Résultats

- Si Site Recovery Manager a correctement appliqué les mappages d'inventaire aux machines virtuelles protégées, l'état de protection du groupe de protection est correct.
- 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 correct.

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 Web Client, sélectionnez **Récupération de site > Plans de récupération**.
- 2 Sous l'onglet **Objets**, cliquez sur l'icône pour créer un plan de récupération.

- 3 Saisissez un nom et une description pour le plan, sélectionnez un dossier, puis cliquez sur **Suivant**.
- 4 Sélectionnez le site de récupération et cliquez sur **Suivant**.
- 5 Sélectionnez le type du groupe dans le menu.

Option	Description
Groupes de protection VM	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.

La valeur par défaut est **Groupes de protection VM**.

Note Si vous utilisez un stockage étendu, sélectionnez **Groupes de protection par stratégie de stockage** pour le type de groupe.

- 6 Sélectionnez un ou plusieurs groupes de protection à récupérer, et cliquez sur **Suivant**.
- 7 Cliquez sur la valeur **Réseau de test**, sélectionnez un réseau à utiliser lors du test de récupération et cliquez sur **Suivant**.

L'option par défaut consiste à créer un réseau isolé automatiquement.

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

Organiser des plans de récupération dans des dossiers

Vous pouvez créer des dossiers dans lesquels organiser des plans de récupération.

Si vous possédez de nombreux plans de récupération, il est utile de les organiser dans des dossiers. Vous pouvez limiter l'accès aux plans de récupération en les plaçant dans des dossiers et en attribuant des autorisations différentes aux dossiers pour différents utilisateurs ou groupes.

Procédure

- 1 Dans la vue Accueil de vSphere Web Client, cliquez sur **Site Recovery**.
- 2 Développez l'**Arborescence d'inventaire** et cliquez sur **Plans de récupération**.
- 3 Sélectionnez l'onglet **Objets associés** et cliquez sur **Dossiers**.
- 4 Cliquez sur l'icône **Créer un dossier**, entrez un nom pour le dossier, puis cliquez sur **OK**.

- 5 Ajoutez des plans de récupération nouveaux ou existants au dossier.

Option	Description
Créer un plan de récupération	Cliquez avec le bouton droit sur le dossier, puis sélectionnez Créer un plan de récupération .
Ajouter un plan de récupération existant	Sélectionnez les plans de récupération à partir de l'arborescence de l'inventaire et faites les glisser vers le dossier.

- 6 (Facultatif) Pour renommer ou supprimer un dossier, cliquez avec le bouton droit sur le dossier et sélectionnez **Renommer le dossier** ou **Supprimer le dossier**.

Vous ne pouvez supprimer un dossier que s'il est vide.

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 Web Client, sélectionnez **Récupération de site > Plans de récupération**.
- 2 Cliquez avec le bouton droit de la souris sur un plan de récupération et sélectionnez **Modifier le plan**.

Vous pouvez également modifier un plan de récupération en cliquant sur l'icône **Modifier un plan de récupération** dans la vue **Étapes de récupération** dans l'onglet **Surveiller**.
- 3 (Facultatif) Changez le nom ou la description du plan dans la zone de texte **Nom du plan de récupération**, et cliquez sur **Suivant**.
- 4 Sur la page du site de récupération, cliquez sur **Suivant**.

Vous ne pouvez pas modifier le site 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) Cliquez sur le réseau de test pour sélectionner 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 :

- [Désactiver l'accès au client Orchestrator pour les non-administrateurs](#)
- [Configuration de l'accès au système de fichiers du serveur pour les workflows et les actions](#)
- [Définir l'accès aux commandes du système d'exploitation pour les workflows et les actions](#)
- [Définir l'accès du JavaScript aux classes Java](#)
- [Définir la propriété de délai d'expiration personnalisée](#)


Désactiver l'accès au client Orchestrator pour les non-administrateurs

Vous pouvez configurer le serveur Orchestrator de sorte à désactiver l'accès au client Orchestrator pour tous les utilisateurs autres que les membres du groupe d'administrateurs d'Orchestrator.

Par défaut, tous les utilisateurs qui disposent d'autorisations d'exécution peuvent se connecter au client Orchestrator. Toutefois, vous pouvez définir une propriété système de configuration d'Orchestrator afin de limiter l'accès au client Orchestrator aux administrateurs d'Orchestrator.

Important Si la propriété n'est pas configurée, ou si la propriété est définie sur `false`, Orchestrator autorise l'accès au client Orchestrator pour tous les utilisateurs.

Procédure

- 1 Connectez-vous au centre de contrôle en tant que **root**.
- 2 Cliquez sur **Propriétés du système**.
- 3 Cliquez sur l'icône **Ajouter** ()
- 4 Dans la zone de texte **Clé**, entrez `com.vmware.o11n.smart-client-disabled`.

- 5 Dans la zone de texte **Valeur**, entrez **true**.
- 6 (Facultatif) Dans la zone de texte **Description**, entrez **Désactiver la connexion client Orchestrator**.
- 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

Vous avez désactivé l'accès au client Orchestrator pour tous les utilisateurs autres que les membres du groupe d'administrateurs d'Orchestrator.

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

Dans Orchestrator, les workflows et les actions ont un accès limité aux 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 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.

Important Avant de modifier le fichier `js-io-rights.conf`, vous devez arrêter le service du centre de contrôle vRealize Orchestrator. Sinon, le fichier `js-io-rights.conf` restaure sa configuration par défaut. Reportez-vous à [Configurer l'accès au système de fichiers du serveur pour les workflows et les actions](#).

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 lecture (r), écriture (w) et exécution (x).
- Chemin d'accès auquel appliquer les droits.

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
-rwx /etc/vco/app-server/security/
+rx /etc/vco
+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

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 console Linux de vRealize Orchestrator Appliance en tant que **racine**.
- 2 Arrêtez le service de centre de contrôle vRealize Orchestrator.

```
service vco-configurator stop
```

- 3 Accédez à `/etc/vco/app-server`.
- 4 Ouvrez le fichier de configuration `js-io-rights.conf` dans un éditeur de texte.

- 5 Ajoutez les lignes nécessaires au fichier `js-io-rights.conf`.

Par exemple, la ligne suivante refuse les droits d'exécution dans le répertoire `/chemin_vers_dossier/noexec` :

```
-x /chemin_vers_dossier/noexec
```

`/chemin_vers_dossier/noexec` conserve des droits d'exécutions, au contraire de `/chemin_vers_dossier/noexec/bar`. Les deux répertoires restent lisibles et inscriptibles.

- 6 Pour appliquer les modifications, exécutez la commande suivante.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh sync-local
```

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

```
service vco-configurator start
```

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

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

Procédure

- 1 Connectez-vous au centre de contrôle en tant que **root**.
- 2 Cliquez sur **Propriétés du système**.
- 3 Cliquez sur l'icône **Ajouter** (+).
- 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 Redémarrez le serveur Orchestrator.

Résultats

Vous avez accordé des autorisations aux applications Orchestrator pour exécuter des commandes locales dans le système d'exploitation hôte du serveur 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, 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 du système 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 pourraient alors avoir accès à l'ensemble des composants système auxquels l'utilisateur exécutant le serveur Orchestrator a accès. Par conséquent, le moteur JavaScript d'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 Enregistrez le fichier de configuration sous un nom adéquat à un emplacement adéquat.
- 3 Connectez-vous au centre de contrôle en tant que **root**.

4 Cliquez sur **Propriétés du système**.

5 Cliquez sur l'icône **Ajouter** ()

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

7 Dans la zone de texte **Valeur**, saisissez le chemin d'accès de votre fichier de configuration.

8 Dans la zone de texte **Description**, saisissez une description pour la propriété système.

9 Cliquez sur **Ajouter**.

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

Un message indique que vos modifications sont correctement enregistrées.

11 Redémarrez le serveur Orchestrator.

Résultats

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

Définir la propriété de délai d'expiration personnalisée

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

Si le délai d'expiration par défaut a expiré avant l'achèvement de certaines opérations, le journal du serveur Orchestrator contient des erreurs.

```
Operation 'getPropertyContent', durée totale : '5742228' pour 1823 appels, temps
moyen : '3149.0', temps min. : '0', temps max. : '32313' Délai d'expiration,
impossible d'obtenir les informations propriétaires 'info'
com.vmware.vmo.plugin.vi4.model.TimeoutException
```

Procédure

1 Connectez-vous au centre de contrôle en tant que **root**.

2 Cliquez sur **Propriétés du système**.

3 Cliquez sur l'icône **Ajouter** ()

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

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

6 (Facultatif) Entrez une description de la propriété système dans la zone de texte **Description**.

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 délai d'expiration par défaut fixé à 20 000 millisecondes.

Pour aller plus loin

10

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

- Connectez-vous au client Orchestrator, exécutez et planifiez les workflows sur les objets d'inventaire vCenter Server ou d'autres objets auxquels Orchestrator a accès via ses plug-ins. Consultez le chapitre *Utilisation du client VMware vRealize Orchestrator*.
- Dupliquez et modifiez les workflows standard d'Orchestrator et écrivez vos propres actions et workflows pour automatiser les opérations dans vCenter Server.
- Développez des plug-ins et des services Web pour étendre la plate-forme Orchestrator.
- Exécutez des workflows sur vos objets d'inventaire vSphere à l'aide de vSphere Web Client.

Ce chapitre contient les rubriques suivantes :

- [Se connecter au client Orchestrator à partir de la console Web du dispositif Orchestrator](#)

Se connecter au client Orchestrator à partir de la console Web du dispositif Orchestrator

Vous devez vous connecter à l'interface du client Orchestrator pour effectuer des tâches d'administration générale ou pour modifier ou créer des workflows.

L'interface du client Orchestrator est conçue pour les développeurs disposant de droits administratifs et souhaitant développer des workflows, des actions et d'autres éléments personnalisés.

Important Vérifiez que les horloges du Orchestrator Appliance et la machine client Orchestrator sont synchronisés.

Conditions préalables

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

- Installez Java 64 bits sur le poste de travail sur lequel vous exécuterez le client Orchestrator.

Note Java 32 bits n'est pas pris en charge

Procédure

- 1 Dans un navigateur Web, entrez l'adresse IP de la machine virtuelle de votre dispositif Orchestrator Appliance.

`http://orchestrator_appliance_ip`

- 2 Cliquez sur **Démarrer le client Orchestrator**.

- 3 Entrez l'adresse IP ou le nom de domaine du Orchestrator Appliance dans la zone de texte **Nom d'hôte**.

L'adresse IP du Orchestrator Appliance s'affiche par défaut.

- 4 Connectez-vous à l'aide du nom d'utilisateur et du mot de passe du client Orchestrator.

Selon que vous utilisez vRealize Automation ou vSphere comme fournisseur d'authentification, entrez les informations d'identification correspondantes pour vous connecter au client Orchestrator.

Si la fonctionnalité de mutualisation est activée sur votre environnement Orchestrator, entrez respectivement le nom d'utilisateur de l'administrateur système ou de l'administrateur de locataires, son mot de passe et son ID de locataire.

- 5 Dans la fenêtre **Avertissement de sécurité**, sélectionnez une option pour gérer l'avertissement de certificat.

Le client Orchestrator communique avec le serveur Orchestrator à l'aide d'un certificat SSL. Une autorité de certification approuvée ne signe pas le certificat pendant l'installation. Vous recevez un avertissement de certificat à chaque fois que vous vous connectez au serveur Orchestrator.

Option	Description
Ignorer	Continuez avec le certificat SSL actuel. Le message d'avertissement s'affichera à nouveau lorsque vous vous reconnecterez au même serveur Orchestrator ou lorsque vous essaierez de synchroniser un workflow avec un serveur Orchestrator distant.
Annuler	Fermez la fenêtre et arrêtez le processus de connexion.
Installer ce certificat et ne plus afficher aucun avertissement de sécurité pour ce serveur.	Cochez cette case et cliquez sur Ignorer pour installer le certificat et ne plus recevoir les avertissements de sécurité.

Vous pouvez remplacer le certificat SSL par défaut par un certificat signé par une autorité de certification. Pour plus d'informations sur la modification des certificats SSL, reportez-vous au guide *Installation et configuration de VMware vRealize Orchestrator*.

Étape suivante

Vous pouvez importer un module, démarrer un workflow ou définir des droits d'accès root sur le système.