

Administration de vRealize Automation

21 décembre 2020

vRealize Automation 8.1

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

Table des matières

- 1 Administration de vRealize Automation** 4
- 2 Administration des utilisateurs** 5
 - Activation de groupes Active Directory dans vRealize Automation pour les projets 6
 - Suppression d'utilisateurs dans vRealize Automation 7
 - Modification des rôles d'utilisateur dans vRealize Automation 8
 - Modification des attributions de rôles de groupe dans vRealize Automation 8
 - Présentation des rôles d'utilisateur vRealize Automation 9
- 3 Maintenance de votre dispositif** 23
 - Démarrage et arrêt de vRealize Automation 23
 - Mettre à jour l'attribution DNS pour vRealize Automation 25
 - Activation de la synchronisation de l'heure 26
 - Désactivation de la synchronisation de l'heure 27
 - Réinitialisation du mot de passe racine 28
- 4 Utilisation de configurations de locataires de plusieurs organisations dans vRealize Automation** 30
 - Configurer la mutualisation entre plusieurs organisations pour vRealize Automation 33
 - Gestion des certificats et de la configuration DNS dans des déploiements dans plusieurs organisations à nœud unique 35
 - Gestion de la configuration des certificats et de DNS sous des déploiements vRealize Automation en cluster 37
 - Connexion aux locataires et ajout d'utilisateurs dans vRealize Automation 40
 - Utilisation de vRealize Orchestrator avec des déploiements vRealize Automation à plusieurs organisations 41
- 5 Utilisation des journaux** 42
 - Utilisation des journaux et des bundles de journaux 42
 - Configuration du transfert de journaux vers vRealize Log Insight 44
 - Comment créer ou mettre à jour une intégration syslog 48
 - Comment supprimer une intégration syslog pour la journalisation 49
- 6 Participation au Programme d'amélioration du produit** 51
 - Rejoindre ou quitter le programme 51
 - Configuration de l'heure de collecte des données pour le programme 52

Administration de vRealize Automation

1

Ce guide explique comment surveiller et gérer les aspects critiques de l'infrastructure et de la gestion des utilisateurs d'un déploiement vRealize Automation.

Les tâches décrites dans ce document sont essentielles pour maintenir un bon niveau opérationnel d'un déploiement vRealize Automation. Ces tâches incluent la gestion des utilisateurs et des groupes, ainsi que la surveillance des journaux système.

Il indique également comment configurer et gérer des déploiements dans plusieurs organisations.

Bien que certaines tâches d'administration de vRealize Automation soient effectuées dans vRealize Automation, d'autres tâches nécessitent l'utilisation de produits associés, tels que vRealize Suite Lifecycle Manager et Workspace ONE Access. Les utilisateurs doivent se familiariser avec ces produits et leurs fonctionnalités avant d'exécuter les tâches applicables.

Par exemple, pour plus d'informations sur la sauvegarde, la restauration et la récupération d'urgence, consultez la section **Sauvegarde, restauration et récupération d'urgence > 2019** de la [documentation du produit vRealize Suite](#).

Note La récupération d'urgence est prise en charge dans vRealize Automation 8.0.1 et versions ultérieures.

Pour plus d'informations sur l'installation, la mise à niveau et la gestion de vRealize Suite Lifecycle Manager, consultez la [documentation du produit Lifecycle Manager](#).

Administration des utilisateurs et des groupes dans vRealize Automation

2

vRealize Automation utilise VMware Workspace ONE Access, l'application de gestion des identités de VMware, pour importer et gérer les utilisateurs et les groupes. Une fois que les utilisateurs et les groupes sont importés ou créés, vous pouvez gérer les attributions de rôles pour les déploiements à locataire unique sur la page Gestion des identités et des accès.

vRealize Automation est installé à l'aide de VMware Lifecycle Manager (vRSLCM ou LCM). Lors de l'installation de vRealize Automation, vous devez importer une instance de Workspace ONE Access existante ou en déployer une nouvelle pour prendre en charge la gestion des identités. Ces deux scénarios définissent vos options de gestion.

- Si vous déployez une nouvelle instance de Workspace ONE Access, vous pouvez gérer les utilisateurs et les groupes via LCM. Lors de l'installation, vous pouvez configurer une connexion Active Directory à l'aide de Workspace ONE Access. Vous pouvez également utiliser la page Gestion des identités et des accès pour afficher et modifier certains aspects des utilisateurs et des groupes dans vRealize Automation, comme décrit dans le présent document.
- Si vous utilisez une instance de Workspace ONE Access existante, importez-la pour l'utiliser avec vRealize Automation via LCM lors de l'installation. Dans ce cas, vous pouvez continuer à utiliser Workspace ONE Access pour gérer les utilisateurs et les groupes, ou bien utiliser les fonctions de gestion de LCM.

Pour plus d'informations sur la gestion des utilisateurs dans un déploiement à plusieurs organisations, consultez [Connexion aux locataires et ajout d'utilisateurs dans vRealize Automation](#).

Vous devez attribuer des rôles aux utilisateurs de vRealize Automation. Les rôles déterminent l'accès aux fonctionnalités dans l'application. Lorsque vous installez vRealize Automation avec une instance de Workspace ONE Access, une organisation par défaut est créée et le rôle de propriétaire de l'organisation est attribué au programme d'installation. Tous les autres rôles vRealize Automation sont attribués par le propriétaire de l'organisation.

Il existe trois types de rôles dans vRealize Automation : les rôles d'organisation, les rôles de service et les rôles de projet. Pour vRealize Automation Cloud Assembly, Service Broker et Code Stream, les rôles de niveau utilisateur peuvent généralement utiliser des ressources, alors que les rôles de niveau administrateur sont requis pour créer et configurer des ressources. Les rôles

d'organisation définissent les autorisations dans le locataire. Les propriétaires de l'organisation possèdent des autorisations de niveau administrateur, alors que les membres de l'organisation disposent d'autorisations de niveau utilisateur. Les propriétaires de l'organisation peuvent ajouter et gérer d'autres utilisateurs.

Rôles d'organisation	Rôles de service
<ul style="list-style-type: none"> ■ Propriétaire d'organisation ■ Membre d'organisation 	<ul style="list-style-type: none"> ■ Administrateur de Cloud Assembly ■ Utilisateur de Cloud Assembly ■ Observateur de Cloud Assembly ■ Administrateur de Service Broker ■ Utilisateur de Service Broker ■ Observateur de Service Broker ■ Administrateur de Code Stream ■ Utilisateur de Code Stream ■ Visualisation de Code Stream

En outre, il existe deux rôles de niveau projet principaux qui ne sont pas affichés dans le tableau : administrateur de projet et utilisateur de projet. Ces rôles sont attribués ad hoc pour chaque projet avec Cloud Assembly. Ces rôles sont assez fluides. Le même utilisateur peut être administrateur sur un projet et utilisateur sur un autre projet. Pour plus d'informations, reportez-vous à la section [Présentation des rôles d'utilisateur vRealize Automation](#).

Pour plus d'informations sur l'utilisation de LCM et de Workspace ONE Access, reportez-vous à [Gestion des utilisateurs avec VMware Identity Manager](#).

Ce chapitre contient les rubriques suivantes :

- [Activation de groupes Active Directory dans vRealize Automation pour les projets](#)
- [Suppression d'utilisateurs dans vRealize Automation](#)
- [Modification des rôles d'utilisateur dans vRealize Automation](#)
- [Modification des attributions de rôles de groupe dans vRealize Automation](#)
- [Présentation des rôles d'utilisateur vRealize Automation](#)

Activation de groupes Active Directory dans vRealize Automation pour les projets

Si un groupe n'est pas disponible sur la page Ajouter des groupes lorsque vous ajoutez des utilisateurs à des projets, consultez la page Gestion des identités et des accès. Si le groupe est disponible, ajoutez-le. S'il n'est pas répertorié sur la page Gestion des identités et des accès de vRealize Automation, il n'est peut-être pas synchronisé dans votre instance de Workspace ONE Access. Assurez-vous qu'il a été synchronisé, puis utilisez cette procédure pour ajouter le groupe.

Vous ne pouvez ajouter des membres d'un groupe Active Directory à un projet que si le groupe est synchronisé avec votre instance de Workspace ONE Access et a été ajouté à l'organisation.

Conditions préalables

Si les groupes ne sont pas synchronisés, ils ne sont pas disponibles lorsque vous tentez de les ajouter à un projet. Vérifiez que vous avez synchronisé vos groupes Active Directory avec votre instance de Lifecycle Manager.

Procédure

- 1 Connectez-vous à vRealize Automation en tant qu'utilisateur du domaine Active Directory que vous ajoutez. Par exemple, @mycompany.com
- 2 Dans Cloud Assembly, cliquez sur Gestion des identités et des accès dans le menu de navigation d'en-tête de droite.
- 3 Cliquez sur **Groupes d'entreprise**, puis sur **Attribuer des rôles**.
- 4 Utilisez la fonction de recherche pour rechercher le groupe que vous ajoutez et sélectionnez-le.
- 5 Attribuez un rôle d'organisation.

Le groupe doit disposer d'au moins un rôle de membre de l'organisation. Pour plus d'informations, reportez-vous à [Présentation des rôles d'utilisateur de vRealize Automation Cloud Assembly](#).
- 6 Cliquez sur **Ajouter un accès au service**, ajoutez un ou plusieurs services et sélectionnez un rôle pour chacun d'entre eux.
- 7 Cliquez sur **Attribuer**.

Résultats

Vous pouvez maintenant ajouter le groupe Active Directory à un projet.

Suppression d'utilisateurs dans vRealize Automation

Vous pouvez supprimer des utilisateurs dans vRealize Automation, si nécessaire.

Tous les utilisateurs sont répertoriés par défaut et vous ne pouvez pas ajouter d'utilisateurs avec la page Gestion des identités et des accès. Vous pouvez supprimer des utilisateurs.

Procédure

- 1 Sélectionnez l'onglet Utilisateurs actifs sur la page Gestion des identités et des accès.
- 2 Localisez et sélectionnez les utilisateurs à supprimer.
- 3 Cliquez sur **Supprimer des utilisateurs**.

Résultats

Les utilisateurs sélectionnés sont supprimés.

Modification des rôles d'utilisateur dans vRealize Automation

Vous pouvez modifier les rôles attribués aux utilisateurs de Workspace ONE Access qui ont été importés dans vRealize Automation.

Conditions préalables

Procédure

- 1 Dans Cloud Assembly, cliquez sur Gestion des identités et des accès dans le menu de navigation d'en-tête de droite.
- 2 Sélectionnez l'utilisateur souhaité dans l'onglet Utilisateurs actifs, puis cliquez sur **Modifier les rôles**.
- 3 Vous pouvez modifier les rôles d'organisation et de service de l'utilisateur.
 - Sélectionnez le menu déroulant en regard de l'en-tête Attribuer des rôles d'organisation pour modifier la relation de l'utilisateur avec l'organisation.
 - Cliquez sur Ajouter un accès au service pour ajouter de nouveaux rôles de service à l'utilisateur.
 - Pour supprimer des rôles d'utilisateurs, cliquez sur le X en regard du service applicable.
- 4 Cliquez sur **Enregistrer**.

Résultats

L'attribution de rôle d'utilisateur est mise à jour comme spécifié.

Modification des attributions de rôles de groupe dans vRealize Automation

Vous pouvez modifier les attributions de rôles pour les groupes dans vRealize Automation.

Conditions préalables

Les utilisateurs et les groupes ont été importés à partir d'une instance de vIDM valide qui est associée à votre déploiement vRealize Automation.

Procédure

- 1 Dans Cloud Assembly, cliquez sur Gestion des identités et des accès dans le menu de navigation d'en-tête de droite.
- 2 Sélectionnez l'onglet Groupes d'entreprises.
- 3 Entrez le nom du groupe pour lequel vous souhaitez modifier les attributions de rôles dans le champ de recherche.

4 Modifiez les attributions de rôles pour le groupe sélectionné. Vous avez le choix entre deux options :

- Attribuer des rôles d'organisation
- Attribuer des rôles de service

5 Cliquez sur **Attribuer**.

Résultats

Les attributions de rôles sont mises à jour comme spécifié.

Présentation des rôles d'utilisateur vRealize Automation

En tant que propriétaire de l'organisation, vous pouvez attribuer aux utilisateurs des rôles d'organisation et des rôles de service. Les rôles déterminent ce que les utilisateurs peuvent faire ou voir. Ensuite, dans les services, l'administrateur de services peut attribuer des rôles de projet. Pour déterminer le rôle que vous souhaitez attribuer, évaluez les tâches dans les tableaux suivants.

Rôles de service Cloud Assembly

Les rôles de service vRealize Automation Cloud Assembly déterminent ce que vous pouvez voir et faire dans vRealize Automation Cloud Assembly. Ces rôles de service sont définis dans la console par un propriétaire d'organisation.

Tableau 2-1. Description des rôles de service vRealize Automation Cloud Assembly

Rôle	Description
Administrateur de Cloud Assembly	Doit disposer d'un accès en lecture et en écriture à l'intégralité de l'interface utilisateur et des ressources API. Seul ce rôle d'utilisateur permet de tout afficher et d'exécuter toutes les opérations : ajouter des comptes de cloud, créer des projets, attribuer un administrateur de projet, etc.
Utilisateur de Cloud Assembly	Un utilisateur ne disposant pas du rôle d'administrateur de Cloud Assembly. Dans un projet vRealize Automation Cloud Assembly, l'administrateur ajoute des utilisateurs aux projets en tant que membres du projet. L'administrateur peut également ajouter un administrateur de projet. Les autorisations pour ces deux rôles sont définies ci-dessous.
Observateur de Cloud Assembly	Utilisateur qui peut voir des informations, mais qui ne peut pas créer, mettre à jour ou supprimer des valeurs. Ce rôle est en lecture seule.

Outre les rôles de service, vRealize Automation Cloud Assembly a des rôles de projet.

Les rôles de projet sont définis dans vRealize Automation Cloud Assembly et peuvent varier d'un projet à l'autre.

Dans les tableaux suivants, qui vous indiquent ce que les différents rôles de service et de projet peuvent voir et faire, notez que les administrateurs de service disposent d'une autorisation complète sur toutes les zones de l'interface utilisateur.

Les descriptions des rôles de projet vous aideront à déterminer les autorisations à accorder à vos utilisateurs.

- Les administrateurs de projet exploitent l'infrastructure créée par l'administrateur de service pour s'assurer que leurs membres de projet disposent des ressources dont ils ont besoin pour leur travail de développement.
- Les membres de projet travaillent dans leurs projets pour concevoir et déployer des Blueprints.
- Les observateurs de projet sont limités à un accès en lecture seule, sauf dans certains cas où ils peuvent effectuer des opérations non destructrices telles que télécharger des Blueprints.

Tableau 2-2. Rôles de service et rôles de projet vRealize Automation Cloud Assembly

Contexte de l'interface utilisateur	Tâche	Administrateur de Cloud Assembly	Observateur de Cloud Assembly	Utilisateur de Cloud Assembly		
				L'utilisateur doit être un administrateur ou un membre de projet pour afficher et exécuter des tâches liées au projet.		
				Administrateur de projet	Membre du projet	Observateur de projet
Accéder à Cloud Assembly						
Console	Dans la console de vRA, vous pouvez voir et ouvrir Cloud Assembly	Oui	Oui	Oui	Oui	Oui
Infrastructure						
	Voir et ouvrir l'onglet Infrastructure	Oui	Oui	Oui	Oui	Oui
Configurer - Projets	Créer des projets	Oui				
	Mettez à jour ou supprimez des valeurs du résumé du projet, des utilisateurs, du provisionnement, Kubernetes, des intégrations et des configurations du projet de test.	Oui		Oui. Vos projets		

Tableau 2-2. Rôles de service et rôles de projet vRealize Automation Cloud Assembly (suite)

Contexte de l'interface utilisateur	Tâche	Administrateur de Cloud Assembly	Observateur de Cloud Assembly	Utilisateur de Cloud Assembly		
				L'utilisateur doit être un administrateur ou un membre de projet pour afficher et exécuter des tâches liées au projet.		
				Administrateur de projet	Membre du projet	Observateur de projet
	Ajoutez des utilisateurs et attribuez des rôles dans des projets.	Oui		Oui. Vos projets.		
	Afficher les projets	Oui	Oui	Oui. Vos projets	Oui. Vos projets	Oui. Vos projets
Configurer - Zones de cloud	Créer, mettre à jour ou supprimer des zones de cloud	Oui				
	Afficher des zones de cloud	Oui	Oui			
Configurer - Zones Kubernetes	Créer, mettre à jour ou supprimer des zones Kubernetes	Oui				
	Afficher des zones Kubernetes	Oui	Oui			
Configurer - Types	Créer, mettre à jour ou supprimer des types	Oui				
	Afficher les types	Oui	Oui			
Configurer - Mappages d'image	Créer, mettre à jour ou supprimer des mappages d'image	Oui				
	Afficher des mappages d'image	Oui	Oui			
Configurer - Profils réseau	Créer, mettre à jour ou supprimer des profils réseau	Oui				

Tableau 2-2. Rôles de service et rôles de projet vRealize Automation Cloud Assembly (suite)

Contexte de l'interface utilisateur	Tâche	Administrateur de Cloud Assembly	Observateur de Cloud Assembly	Utilisateur de Cloud Assembly		
				L'utilisateur doit être un administrateur ou un membre de projet pour afficher et exécuter des tâches liées au projet.		
				Administrateur de projet	Membre du projet	Observateur de projet
	Afficher des profils réseau d'image	Oui	Oui			
Configurer - Profils de stockage	Créer, mettre à jour ou supprimer des profils de stockage	Oui				
	Afficher des profils de stockage d'image	Oui	Oui			
Configurer - Cartes de tarification	Créer, mettre à jour ou supprimer des cartes de tarification	Oui				
	Afficher les cartes de tarification	Oui	Oui			
Configurer - Balises	Créer, mettre à jour ou supprimer des balises	Oui				
	Afficher des balises	Oui	Oui			
Ressources - Calcul	Ajouter des balises aux ressources de calcul découvertes	Oui				
	Afficher des ressources de calcul découvertes	Oui	Oui			
Ressources - Réseaux	Modifier des balises réseau, des plages d'adresses IP, des adresses IP	Oui				

Tableau 2-2. Rôles de service et rôles de projet vRealize Automation Cloud Assembly (suite)

Contexte de l'interface utilisateur	Tâche	Administrateur de Cloud Assembly	Observateur de Cloud Assembly	Utilisateur de Cloud Assembly		
				L'utilisateur doit être un administrateur ou un membre de projet pour afficher et exécuter des tâches liées au projet.		
				Administrateur de projet	Membre du projet	Observateur de projet
	Afficher les ressources réseau découvertes	Oui	Oui			
Ressources - Sécurité	Ajouter des balises aux groupes de sécurité découverts	Oui				
	Afficher les groupes de sécurité découverts	Oui	Oui			
Ressources - Stockage	Ajouter des balises au stockage découvert	Oui				
	Afficher le stockage	Oui	Oui			
Ressources - Machines	Ajouter et supprimer des machines	Oui				
	Afficher les machines	Oui	Oui	Oui. Vos projets	Oui. Vos projets	Oui. Vos projets
Ressources - Volumes	Supprimer les volumes de stockage découverts	Oui				
	Afficher les volumes de stockage découverts	Oui	Oui	Oui. Vos projets	Oui. Vos projets	Oui. Vos projets.
Ressources - Kubernetes	Déployer ou ajouter des clusters Kubernetes, et créer ou ajouter des espaces de noms	Oui				

Tableau 2-2. Rôles de service et rôles de projet vRealize Automation Cloud Assembly (suite)

Contexte de l'interface utilisateur	Tâche	Administrateur de Cloud Assembly	Observateur de Cloud Assembly	Utilisateur de Cloud Assembly		
				L'utilisateur doit être un administrateur ou un membre de projet pour afficher et exécuter des tâches liées au projet.		
				Administrateur de projet	Membre du projet	Observateur de projet
	Afficher les clusters et les espaces de noms Kubernetes	Oui	Oui	Oui. Vos projets	Oui. Vos projets	Oui. Vos projets
Activité - Demandes	Supprimer les enregistrements de demande de déploiement	Oui				
	Afficher les enregistrements de demande de déploiement	Oui	Oui	Oui. Vos projets	Oui. Vos projets	Oui. Vos projets
Activité - Journaux des événements	Afficher les journaux des événements	Oui	Oui	Oui. Vos projets	Oui. Vos projets	Oui. Vos projets
Connexions - Comptes de cloud	Créer, mettre à jour ou supprimer des comptes de cloud	Oui				
	Afficher les comptes de cloud	Oui	Oui			
Connexions - Intégrations	Créer, mettre à jour ou supprimer des intégrations	Oui				
	Afficher les intégrations	Oui	Oui			
Intégration	Créer, mettre à jour ou supprimer des plans d'intégration	Oui				
	Afficher les plans d'intégration	Oui	Oui			Oui. Vos projets
Marketplace						
	Voir et ouvrir l'onglet Marketplace	Oui	Oui			

Tableau 2-2. Rôles de service et rôles de projet vRealize Automation Cloud Assembly (suite)

Contexte de l'interface utilisateur	Tâche	Administrateur de Cloud Assembly	Observateur de Cloud Assembly	Utilisateur de Cloud Assembly		
				L'utilisateur doit être un administrateur ou un membre de projet pour afficher et exécuter des tâches liées au projet.		
				Administrateur de projet	Membre du projet	Observateur de projet
	Utiliser les Blueprints téléchargés dans l'onglet Blueprints	Oui		Oui. En cas d'association à vos projets.	Oui. En cas d'association à vos projets.	
Marketplace - Blueprints	Télécharger un Blueprint	Oui				
	Afficher les Blueprints	Oui	Oui			
Marketplace - Images	Télécharger les images	Oui				
	Afficher les images	Oui	Oui			
Marketplace - Téléchargements	Afficher le journal de tous les éléments téléchargés	Oui	Oui			
Extensibilité						
	Voir et ouvrir l'onglet Extensibilité	Oui	Oui			Oui
Événements	Afficher les événements d'extensibilité	Oui	Oui			
Abonnements	Créer, mettre à jour ou supprimer les abonnements d'extensibilité	Oui				
	Désactiver les abonnements	Oui				
	Afficher les abonnements	Oui	Oui			
Bibliothèque - Rubriques d'événements	Afficher les rubriques d'événements	Oui	Oui			

Tableau 2-2. Rôles de service et rôles de projet vRealize Automation Cloud Assembly (suite)

Contexte de l'interface utilisateur	Tâche	Administrateur de Cloud Assembly	Observateur de Cloud Assembly	Utilisateur de Cloud Assembly		
				L'utilisateur doit être un administrateur ou un membre de projet pour afficher et exécuter des tâches liées au projet.		
				Administrateur de projet	Membre du projet	Observateur de projet
Bibliothèque - Actions	Créer, mettre à jour ou supprimer des actions d'extensibilité	Oui				
	Afficher les actions d'extensibilité	Oui	Oui			
Bibliothèque - Workflows	Afficher les workflows d'extensibilité	Oui	Oui			
Activité - Exécutions d'actions	Annuler ou supprimer les exécutions d'actions d'extensibilité	Oui				
	Afficher les exécutions d'actions d'extensibilité	Oui	Oui			Oui. Vos projets
Activité - Exécutions de workflows	Afficher les exécutions de workflows d'extensibilité	Oui	Oui			
Concevoir						
Concevoir	Ouvrir l'onglet Concevoir et afficher une liste de Blueprints	Oui	Oui	Oui. Vos projets	Oui. Vos projets	Oui. Vos projets
Blueprints	Créer, mettre à jour et supprimer des Blueprints	Oui		Oui. Vos projets	Oui. Vos projets	
	Afficher les Blueprints	Oui	Oui	Oui. Vos projets	Oui. Vos projets	Oui. Vos projets
	Télécharger les Blueprints	Oui	Oui	Oui. Vos projets	Oui. Vos projets	Oui. Vos projets
	Télécharger des Blueprints	Oui		Oui. Vos projets	Oui. Vos projets	
	Déployer des Blueprints	Oui		Oui. Vos projets	Oui. Vos projets	

Tableau 2-2. Rôles de service et rôles de projet vRealize Automation Cloud Assembly (suite)

Contexte de l'interface utilisateur	Tâche	Administrateur de Cloud Assembly	Observateur de Cloud Assembly	Utilisateur de Cloud Assembly		
				L'utilisateur doit être un administrateur ou un membre de projet pour afficher et exécuter des tâches liées au projet.		
				Administrateur de projet	Membre du projet	Observateur de projet
	Version et restaurer des Blueprints	Oui		Oui. Vos projets	Oui. Vos projets	
	Publier des Blueprints dans le catalogue	Oui		Oui. Vos projets		
Ressources personnalisées	Créer, mettre à jour ou supprimer des ressources personnalisées	Oui				
	Afficher les ressources personnalisées	Oui	Oui	Oui. Vos projets	Oui. Vos projets	Oui. Vos projets
Actions personnalisées	Créer, mettre à jour ou supprimer des actions personnalisées	Oui				
	Afficher les actions personnalisées	Oui	Oui	Oui. Vos projets	Oui. Vos projets	Oui. Vos projets
Déploiements						
	Voir et ouvrir l'onglet Déploiements	Oui	Oui	Oui	Oui	Oui
	Afficher les déploiements, y compris les détails du déploiement, l'historique du déploiement et les informations de dépannage.	Oui	Oui	Oui. Vos projets	Oui. Vos projets	Oui. Vos projets
	Exécuter les actions du jour 2 sur les déploiements en fonction des stratégies	Oui		Oui. Vos projets	Oui. Vos projets	

Rôles de service Service Broker

Les rôles de service vRealize Automation Service Broker déterminent ce que vous pouvez voir et faire dans vRealize Automation Service Broker. Ces rôles de service sont définis dans la console par un propriétaire d'organisation.

Tableau 2-3. Description des rôles de service Service Broker

Rôle	Description
Administrateur de Service Broker	Doit disposer d'un accès en lecture et en écriture à l'intégralité de l'interface utilisateur et des ressources API. Seul ce rôle d'utilisateur permet de réaliser toutes les tâches, notamment de créer un projet et d'attribuer un administrateur de projet.
Utilisateur de Service Broker	Tout utilisateur ne disposant pas du rôle d'administrateur de vRealize Automation Service Broker. Dans un projet vRealize Automation Service Broker, l'administrateur ajoute des utilisateurs aux projets en tant que membres du projet. L'administrateur peut également ajouter un administrateur de projet. Les autorisations pour ces deux rôles sont définies ci-dessous.
Observateur de Service Broker	Utilisateur disposant d'autorisations en lecture seule qui peut voir des informations, mais qui ne peut pas créer, mettre à jour ou supprimer des valeurs.

Outre les rôles de service, vRealize Automation Service Broker a des rôles de projet.

Les rôles de projet sont définis dans vRealize Automation Service Broker et peuvent varier d'un projet à l'autre.

Dans les tableaux suivants, qui vous indiquent ce que les différents rôles de service et de projet peuvent voir et faire, notez que les administrateurs de service disposent d'une autorisation complète sur toutes les zones de l'interface utilisateur.

Utilisez les descriptions suivantes des rôles du projet pour vous aider à déterminer les autorisations à accorder à vos utilisateurs.

- Les administrateurs de projet exploitent l'infrastructure créée par l'administrateur de service pour s'assurer que leurs membres de projet disposent des ressources dont ils ont besoin pour leur travail de développement.
- Les membres de projet travaillent dans leurs projets pour concevoir et déployer des Blueprints.
- Les observateurs de projet sont limités à un accès en lecture seule.

Tableau 2-4. Rôles du Service Broker et rôles de projet

Contexte de l'interface utilisateur	Tâche	Administrateur de Service Broker	Observateur de Service Broker	Utilisateur de Service Broker L'utilisateur doit être un administrateur de projet pour voir et effectuer des tâches liées au projet.		
				Administrateur de projet	Membre du projet	Observateur de projet
Accéder à Service Broker						
Console	Dans la console, vous pouvez voir et ouvrir Service Broker	Oui	Oui	Oui	Oui	Oui
Infrastructure						
	Voir et ouvrir l'onglet Infrastructure	Oui	Oui			
Configurer - Projets	Créer des projets	Oui				
	Mettre à jour ou supprimer des valeurs du résumé du projet, des utilisateurs, du provisionnement, des Kubernetes et des intégrations	Oui				
	Afficher les projets	Oui	Oui			
Configurer - Zones de cloud	Créer, mettre à jour ou supprimer des zones de cloud	Oui				
	Afficher des zones de cloud	Oui	Oui			
Configurer - Zones Kubernetes	Créer, mettre à jour ou supprimer des zones Kubernetes	Oui				
	Afficher des zones Kubernetes	Oui	Oui			
Connexions - Comptes de cloud	Créer, mettre à jour ou supprimer des comptes de cloud	Oui				
	Afficher les comptes de cloud	Oui	Oui			

Tableau 2-4. Rôles du Service Broker et rôles de projet (suite)

Contexte de l'interface utilisateur	Tâche	Administrateur de Service Broker	Observateur de Service Broker	Utilisateur de Service Broker L'utilisateur doit être un administrateur de projet pour voir et effectuer des tâches liées au projet.		
				Administrateur de projet	Membre du projet	Observateur de projet
Connexions - Intégrations	Créer, mettre à jour ou supprimer des intégrations	Oui				
	Afficher les intégrations	Oui	Oui			
Activité - Demandes	Supprimer les enregistrements de demande de déploiement	Oui				
	Afficher les enregistrements de demande de déploiement	Oui				
Activité - Journaux des événements	Afficher les journaux des événements	Oui				
Contenu et stratégies						
	Voir et ouvrir l'onglet Contenu et stratégies	Oui	Oui			
Sources de contenu	Créer, mettre à jour ou supprimer des sources de contenu	Oui				
	Afficher les sources de contenu	Oui	Oui			
Partage de contenu	Ajouter ou supprimer du contenu partagé	Oui				
	Afficher le contenu partagé	Oui	Oui			
Contenu	Personnaliser un formulaire et configurer un élément	Oui				
	Afficher le contenu	Oui	Oui			

Tableau 2-4. Rôles du Service Broker et rôles de projet (suite)

Contexte de l'interface utilisateur	Tâche	Administrateur de Service Broker	Observateur de Service Broker	Utilisateur de Service Broker L'utilisateur doit être un administrateur de projet pour voir et effectuer des tâches liées au projet.		
				Administrateur de projet	Membre du projet	Observateur de projet
Stratégies - Définitions	Créer, mettre à jour ou supprimer des définitions de stratégie	Oui				
	Afficher les définitions de stratégie	Oui	Oui			
Stratégies - Application	Afficher le journal d'application	Oui	Oui			
Notifications - Serveur de messagerie	Configurer un serveur de messagerie	Oui				
Catalogue						
	Voir et ouvrir l'onglet Catalogue	Oui	Oui	Oui	Oui	Oui
	Afficher les éléments de catalogue disponibles	Oui	Oui	Oui. Vos projets	Oui. Vos projets	Oui. Vos projets
	Demander un élément de catalogue	Oui		Oui. Vos projets	Oui. Vos projets	
Déploiements						
	Voir et ouvrir l'onglet Déploiements	Oui	Oui	Oui.	Oui	Oui
	Afficher les déploiements, y compris les détails du déploiement, l'historique du déploiement et les informations de dépannage.	Oui	Oui	Oui. Vos projets	Oui. Vos projets	Oui. Vos projets

Tableau 2-4. Rôles du Service Broker et rôles de projet (suite)

Contexte de l'interface utilisateur	Tâche	Administrateur de Service Broker	Observateur de Service Broker	Utilisateur de Service Broker L'utilisateur doit être un administrateur de projet pour voir et effectuer des tâches liées au projet.		
				Administrateur de projet	Membre du projet	Observateur de projet
	Exécuter les actions du jour 2 sur les déploiements en fonction des stratégies	Oui		Oui. Vos projets	Oui. Vos projets	
Approbations						
	Voir et ouvrir l'onglet Approbations	Oui	Oui	Oui	Oui	Oui
	Répondre aux demandes d'approbation	Oui		Rôle d'utilisateur Service Broker uniquement	Rôle d'utilisateur Service Broker uniquement	Rôle d'utilisateur Service Broker uniquement

Maintenance de votre dispositif vRealize Automation

3

En tant qu'administrateur système, vous devrez peut-être effectuer diverses tâches pour garantir le bon fonctionnement de votre application vRealize Automation installée.

Si vous venez de commencer à utiliser vRealize Automation, ces tâches ne sont pas requises. Le fait de savoir effectuer ces tâches est utile si vous devez résoudre des problèmes de performances ou de comportement du produit.

Ce chapitre contient les rubriques suivantes :

- [Démarrage et arrêt de vRealize Automation](#)
- [Mettre à jour l'attribution DNS pour vRealize Automation](#)
- [Activation de la synchronisation de l'heure avec vRealize Automation](#)
- [Désactivation de la synchronisation de l'heure](#)
- [Réinitialisation du mot de passe racine pour vRealize Automation](#)

Démarrage et arrêt de vRealize Automation

Observez les procédures appropriées lors du démarrage ou de l'arrêt de vRealize Automation.

Arrêter vRealize Automation

Pour préserver l'intégrité des données, arrêtez les services vRealize Automation avant de mettre hors tension les dispositifs virtuels.

Note Si possible, évitez d'utiliser la commande `vracli reset vidm`. Cette commande réinitialise toute la configuration de Workspace One Access et rompt l'association entre les utilisateurs et les ressources provisionnées.

- 1 Connectez-vous à la console de n'importe quel dispositif vRealize Automation au moyen de SSH ou de VMRC.

- 2 Pour arrêter les services vRealize Automation sur tous les nœuds de cluster, exécutez l'ensemble de commandes suivant.

Note Si vous copiez certaines de ces commandes à exécuter et qu'elles échouent, collez-les d'abord dans le bloc-notes, puis copiez-les à nouveau avant de les exécuter. Cette procédure supprime tous les caractères masqués et autres artefacts susceptibles d'être présents dans la source de la documentation.

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

- 3 Arrêtez les dispositifs vRealize Automation.

Votre déploiement de vRealize Automation est maintenant arrêté.

Démarrer vRealize Automation

À la suite d'un arrêt non planifié, d'un arrêt contrôlé ou d'une procédure de récupération, vous devez redémarrer les composants vRealize Automation dans un ordre spécifique. vRLCM est un composant non critique, vous pouvez donc le démarrer à tout moment. Les composants VMware Workspace ONE Access, auparavant VMware Identity Management, doivent être démarrés avant de démarrer vRealize Automation.

Note Vérifiez que les équilibrages de charge applicables sont en cours d'exécution avant de démarrer les composants vRealize Automation.

- 1 Mettez sous tension tous les dispositifs vRealize Automation et attendez qu'ils démarrent.
- 2 Connectez-vous à la console pour tout dispositif au moyen de SSH ou de VMRC, et exécutez la commande suivante pour restaurer les services sur tous les nœuds.

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

- 3 Vérifiez que tous les services sont en cours d'exécution avec la commande suivante.

```
kubectl get pods --all-namespaces
```

Note Vous devez voir trois instances de chaque service et elles doivent se trouver à l'état En cours d'exécution ou Terminé.

Lorsque tous les services sont répertoriés comme En cours d'exécution ou Terminé, vRealize Automation est prêt à être utilisé.

Redémarrer vRealize Automation

Vous pouvez redémarrer tous les services vRealize Automation de manière centralisée depuis n'importe quel dispositif de votre cluster. Suivez les instructions précédentes pour arrêter vRealize Automation, puis utilisez les instructions pour démarrer vRealize Automation. Avant de redémarrer vRealize Automation, vérifiez que tous les équilibres de charge et tous les composants VMware Workspace ONE Access applicables sont en cours d'exécution.

Lorsque tous les services sont répertoriés comme En cours d'exécution ou Terminé, vRealize Automation est prêt à être utilisé.

Exécutez la commande suivante pour vérifier que tous les services sont en cours d'exécution :

```
kubect1 -n prelude get pods
```

Mettre à jour l'attribution DNS pour vRealize Automation

Un administrateur peut mettre à jour les attributions DNS pour vRealize Automation.

Procédure

- 1 Connectez-vous à la console de n'importe quel dispositif vRealize Automation au moyen de SSH ou de VMRC.
- 2 Pour arrêter les services vRealize Automation sur tous les nœuds de cluster, exécutez l'ensemble de commandes suivant.

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

- 3 Connectez-vous à vCenter et arrêtez tous les nœuds vRealize Automation à l'aide de la commande Shut Down Guest OS .
- 4 Mettez à jour la propriété OVF DNS pour chaque nœud vRealize Automation.
 - a Accédez au nœud vRealize Automation à partir de l'inventaire vCenter.
 - b Sélectionnez l'onglet Configurer et développez Paramètres.
 - c Sélectionnez Options vApp.
 - d Dans la liste des propriétés OVF, recherchez et sélectionnez vami.DNS.vRealize_Automation.
 - e Cliquez sur **Définir la valeur** et entrez les nouvelles entrées DNS dans la zone de texte Valeur de la propriété.
 - f Cliquez sur **OK**.
- 5 Démarrez tous les nœuds vRealize Automation et attendez qu'ils démarrent complètement, ce qui sera indiqué par un écran bleu sur la console.

- 6 Redémarrez les nœuds vRealize Automation et attendez qu'ils démarrent complètement.
- 7 Connectez-vous à chaque nœud de vRealize Automation avec SSH et vérifiez que les nouveaux serveurs DNS sont répertoriés dans `/etc/resolve.conf`.
- 8 Sur l'un des nœuds vRealize Automation, exécutez la commande suivante pour démarrer les services vRealize Automation : `/opt/scripts/deploy.sh`

Résultats

Les paramètres DNS vRealize Automation sont modifiés comme spécifié.

Activation de la synchronisation de l'heure avec vRealize Automation

Vous pouvez activer la synchronisation de l'heure sur votre déploiement vRealize Automation en utilisant la ligne de commande du dispositif vRealize Automation.

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

Configuration NTP	Description
ESXi	<p>Vous pouvez utiliser cette configuration lorsque le serveur ESXi hébergeant le dispositif vRealize Automation est synchronisé avec un serveur NTP. Si vous utilisez un déploiement en cluster, tous les hôtes ESXi doivent être synchronisés avec un serveur NTP.</p> <p>Note Vous pouvez rencontrer un décalage de l'horloge si votre déploiement vRealize Automation est migré vers un hôte ESXi qui n'est pas synchronisé avec un serveur NTP.</p> <p>Pour plus d'informations sur la configuration de NTP pour ESXi, reportez-vous à l'article 57147 de la base de connaissances Configuration du protocole NTP (Network Time Protocol) sur un hôte ESXi à l'aide de vSphere Web Client.</p>
systemd	<p>Cette configuration utilise le démon <code>systemd-timesyncd</code> pour synchroniser les horloges de votre déploiement vRealize Automation.</p> <p>Note Par défaut, le démon <code>systemd-timesyncd</code> est activé, mais configuré sans serveur NTP. Si le dispositif vRealize Automation utilise une configuration d'adresse IP dynamique, le dispositif peut utiliser n'importe quel serveur NTP reçu par le protocole DHCP.</p>

Procédure

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

2 Activez NTP avec ESXi.

- a Exécutez la commande `vracli ntp esxi`.
- b Exécutez la commande `vracli ntp apply`.

La configuration NTP d'ESXi est appliquée au déploiement vRealize Automation.

3 Activez NTP avec systemd.

- a Exécutez la commande `vracli ntp systemd --set FQDN_or_IP_of_systemd_server`.

Note Vous pouvez ajouter plusieurs serveurs NTP systemd en séparant leurs adresses réseau par une virgule.

- b Exécutez la commande `vracli ntp apply`.

La configuration NTP de systemd est appliquée au déploiement vRealize Automation.

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

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

Désactivation de la synchronisation de l'heure

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

Vous pouvez également réinitialiser la configuration NTP de votre dispositif vRealize Automation en exécutant la commande `vracli ntp reset` et appliquer la nouvelle configuration en exécutant la commande `vracli ntp apply`.

Conditions préalables

Vérifiez que vous avez configuré la synchronisation de l'heure avec ESXi ou systemd. Reportez-vous à la section [Activation de la synchronisation de l'heure avec vRealize Automation](#).

Procédure

- 1** Connectez-vous à la ligne de commande du dispositif vRealize Automation en tant qu'utilisateur **racine**.
- 2** Pour désactiver la synchronisation de l'heure avec ESXi ou systemd, exécutez la commande `vracli ntp disable`.
- 3** Exécutez la commande `vracli ntp apply`.
- 4** (Facultatif) Pour confirmer l'état de la configuration NTP, exécutez la commande `vracli ntp status`.

Réinitialisation du mot de passe racine pour vRealize Automation

Vous pouvez réinitialiser un mot de passe racine vRealize Automation perdu ou oublié.

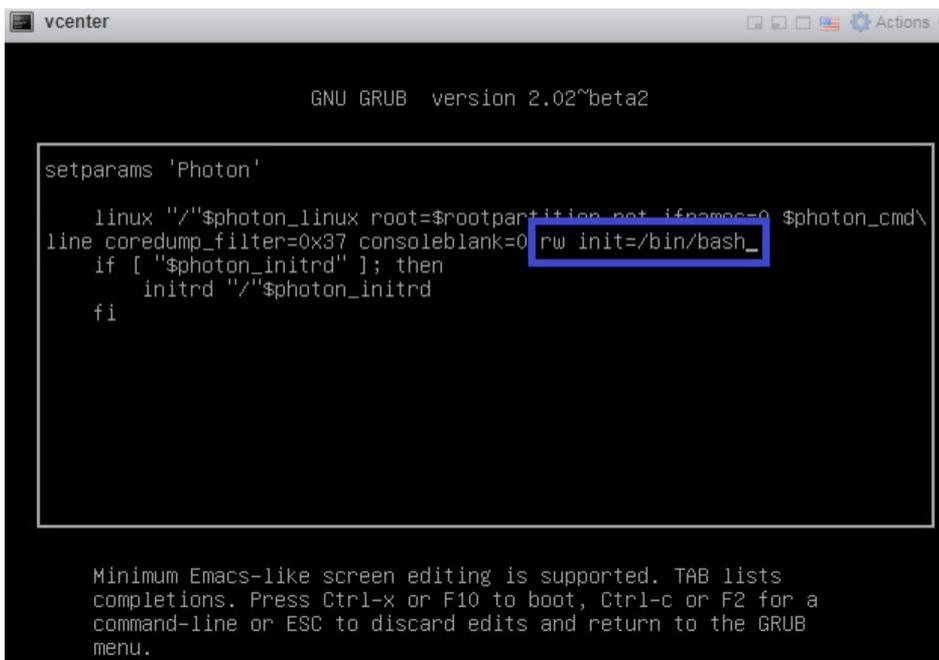
Dans cette procédure, vous devez utiliser une fenêtre de ligne de commande sur le dispositif vCenter hôte pour réinitialiser le mot de passe racine vRealize Automation de votre organisation.

Conditions préalables

Ce processus est destiné aux administrateurs vRealize Automation et nécessite les informations d'identification requises pour accéder au dispositif vCenter hôte.

Procédure

- 1 Arrêter et démarrez vRealize Automation en suivant la procédure décrite dans [Démarrage et arrêt de vRealize Automation](#).
- 2 Lorsque la fenêtre de ligne de commande du système d'exploitation Photon s'affiche, entrez `e` et appuyez sur la touche **Entrée** pour ouvrir l'éditeur du menu de démarrage GNU GRUB.
- 3 Dans l'éditeur GNU GRUB, entrez `rw init=/bin/bash` à la fin de la ligne commençant par `linux` `"/" $photon_linux root=rootpartition` comme indiqué ci-dessous :



```

vcenter
GNU GRUB version 2.02~beta2

setparams 'Photon'

linux "/"$photon_linux root=$rootpartition not_ifnames=0 $photon_cmd\
line coredump_filter=0x37 consoleblank=0 rw init=/bin/bash_
if [ "$photon_initrd" ]; then
  initrd "/"$photon_initrd
fi

Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
command-line or ESC to discard edits and return to the GRUB
menu.

```

- 4 Cliquez sur la touche **F10** pour transférer votre modification et redémarrer vRealize Automation.
- 5 Attendez que vRealize Automation redémarre.
- 6 À l'invite `root [/]#`, entrez `passwd` et appuyez sur la touche **Entrée**.
- 7 À l'invite `New password:`, entrez votre nouveau mot de passe et appuyez sur la touche **Entrée**.

- 8 À l'invite `Retype new password:`, entrez une nouvelle fois votre nouveau mot de passe et appuyez sur la touche **Entrée**.
- 9 À l'invite `root [/]#`, entrez `reboot -f` et appuyez sur la touche **Entrée** pour terminer le processus de réinitialisation du mot de passe racine.

```
root [ / ]# passwd
New password:
Retype new password:
passwd: password updated successfully
root [ / ]# reboot -f_
```

Étape suivante

En tant qu'administrateur vRealize Automation, vous pouvez maintenant vous connecter à vRealize Automation avec le nouveau mot de passe racine.

Utilisation de configurations de locataires de plusieurs organisations dans vRealize Automation

4

vRealize Automation permet aux fournisseurs informatiques clients de configurer plusieurs locataires ou organisations dans chaque déploiement. Les fournisseurs peuvent configurer des organisations à plusieurs locataires et allouer une infrastructure dans chaque déploiement. Les fournisseurs peuvent également gérer les utilisateurs pour les locataires. Chaque locataire gère ses propres projets, ressources et déploiements.

Dans une configuration multi-organisation de vRealize Automation, les fournisseurs peuvent créer plusieurs organisations, et chaque organisation de locataires utilise ses propres projets, ressources et déploiements. Bien que les fournisseurs ne puissent pas gérer l'infrastructure des locataires à distance, ils peuvent se connecter aux locataires et gérer l'infrastructure de leurs locataires.

L'architecture mutualisée repose sur la coordination et la configuration de trois produits VMware, comme indiqué ci-dessous :

- **Workspace ONE Access** : ce produit assure la prise en charge de l'infrastructure pour l'architecture mutualisée et les connexions de domaine Active Directory qui fournissent la gestion des utilisateurs et des groupes dans les organisations de locataires.
- **vRealize Suite Lifecycle Manager** : ce produit prend en charge la création et la configuration de locataires pour les produits pris en charge, tels que vRealize Automation. Il fournit également des fonctionnalités de gestion des certificats.
- **vRealize Automation** : les fournisseurs et les utilisateurs se connectent à vRealize Automation pour accéder aux locataires dans lesquels ils créent et gèrent des déploiements.

Lors de la configuration de l'architecture mutualisée, les utilisateurs doivent se familiariser avec ces trois produits et la documentation qui leur est associée.

Pour plus d'informations sur l'utilisation de LCM et de Workspace ONE Access, consultez [Gestion des utilisateurs avec VMware Identity Manager](#) et [Administration de VMware Workspace ONE Access](#).

Les administrateurs disposant de privilèges vRealize Suite Lifecycle Manager créent et gèrent des locataires à l'aide de la page Lifecycle Manager Tenants située sous le service de gestion des identités et des locataires. Les locataires sont construits à l'aide d'une connexion IWA ou LDAP Active Directory et ils sont pris en charge par l'instance associée de VMware Workspace ONE Access qui est requise pour les déploiements vRealize Automation. Reportez-vous à la documentation associée pour plus d'informations sur l'utilisation de Lifecycle Manager.

Lorsque vous configurez une architecture mutualisée, vous démarrez avec un locataire de base ou le locataire principal. Ce locataire est le locataire par défaut qui est créé lorsque l'application Workspace ONE Access sous-jacente est déployée. Les autres locataires, appelés sous-locataires, peuvent être basés sur le locataire principal. vRealize Automation prend actuellement en charge jusqu'à 20 organisations de locataires avec le déploiement standard à trois nœuds.

Lors de la configuration de vRealize Automation pour la mutualisation, vous devez d'abord installer l'application dans une configuration d'organisation unique, puis utiliser Lifecycle Manager pour établir une configuration à plusieurs organisations. Un déploiement de Workspace ONE Access prend en charge la gestion des locataires et des connexions de domaine Active Directory associées.

Lorsque l'architecture mutualisée est initialement configurée, un administrateur fournisseur est désigné dans Lifecycle Manager. Vous pouvez modifier cette désignation ou ajouter des administrateurs ultérieurement si vous le souhaitez. Dans les configurations à plusieurs organisations, les utilisateurs et les groupes de vRealize Automation sont gérés principalement via Workspace ONE Access.

Une fois les organisations créées, les utilisateurs autorisés peuvent se connecter à leurs applications pour créer ou utiliser des projets et des ressources, et créer des déploiements. Les administrateurs peuvent gérer les rôles d'utilisateur dans vRealize Automation.

Établissement d'une configuration à plusieurs organisations

Vous pouvez activer un déploiement à plusieurs organisations après l'installation d'une instance de vRealize Automation. Lors de la mise en place d'une configuration à plusieurs organisations, vous devez configurer l'instance externe de Workspace ONE Access pour une utilisation mutualisée, puis utiliser Lifecycle Manager pour créer et configurer des locataires. Cela s'applique aux déploiements nouveaux et existants. En tant qu'étape initiale de configuration des locataires, vous devez utiliser Lifecycle Manager pour définir un alias pour le locataire principal qui a été créé par défaut sur Workspace ONE Access. Les sous-locataires que vous créez sur base de ce locataire principal héritent des configurations de domaine Active Directory de ce locataire principal.

Dans Lifecycle Manager, vous attribuez des locataires à un produit (tel que vRealize Automation) et à un environnement spécifique. Lorsque vous configurez un locataire, vous devez également désigner un administrateur de locataire. Par défaut, la mutualisation est activée en fonction du nom d'hôte du locataire. Les utilisateurs peuvent choisir de configurer manuellement le nom du locataire par nom DNS. Au cours de cette procédure, vous devez définir plusieurs indicateurs pour prendre en charge l'architecture mutualisée, et vous devez également configurer l'équilibrage de charge.

Si vous utilisez une instance en cluster, les noms d'hôte Workspace ONE Access et vRealize Automation basés sur le locataire pointeront vers l'équilibrage de charge.

Si vos équilibrages de charge vRealize Automation et Workspace ONE Access en cluster n'utilisent pas de certificats génériques, les utilisateurs doivent ajouter des noms d'hôte de locataires en tant qu'entrées SAN sur les certificats pour chaque locataire créé.

Vous ne pouvez pas supprimer des locataires dans vRealize Automation ou dans Lifecycle Manager. Si vous devez ajouter des locataires à un déploiement mutualisé existant, vous pouvez le faire à l'aide de Lifecycle Manager, mais cela nécessitera une interruption de trois à quatre heures.

Noms d'hôte et architecture mutualisée

Dans les versions antérieures de vRealize Automation, les utilisateurs accédaient aux locataires avec des URL qui étaient basées sur le chemin d'accès au répertoire. Dans l'implémentation mutualisée actuelle, les utilisateurs accèdent aux locataires sur la base du nom d'hôte.

En outre, le format de nom d'hôte que les utilisateurs de vRealize Automation utiliseront pour accéder aux locataires diffère du format utilisé pour accéder aux locataires dans Workspace ONE Access. Par exemple, un nom d'hôte valide a l'aspect suivant : *tenant1.example.eng.vmware.com* par opposition à *vidm-node1.eng.vmware.com*.

Mutualisation et certificats

Vous devez créer des certificats pour tous les composants associés à une configuration à plusieurs organisations. Vous aurez besoin d'un ou de plusieurs certificats pour Workspace ONE Access, Lifecycle Manager et vRealize Automation, selon que vous utilisez une configuration à nœud unique ou une configuration en cluster.

Lors de la configuration des certificats, vous pouvez utiliser des caractères génériques avec des noms SAN ou des noms dédiés. L'utilisation de caractères génériques simplifie la gestion des certificats, car ces derniers doivent être mis à jour chaque fois que vous ajoutez de nouveaux locataires. Si vos équilibrages de charge vRealize Automation et Workspace ONE Access n'utilisent pas de certificats génériques, vous devez ajouter des noms d'hôte de locataires en tant qu'entrées SAN sur les certificats pour chaque nouveau locataire créé. De plus, si vous utilisez SAN, les certificats doivent être mis à jour manuellement si vous ajoutez ou supprimez des hôtes ou si vous modifiez un nom d'hôte. Vous devez également mettre à jour des entrées DNS pour les locataires.

Notez que Lifecycle Manager ne crée pas de certificats distincts pour chaque locataire. Il crée plutôt un certificat unique avec chaque nom d'hôte de locataire répertorié. Pour les configurations de base, le CNAME du locataire utilise le format suivant : *tenantname.vrahostname.domain*. Pour les configurations à haute disponibilité, le nom utilise le format suivant : *tenantname.vraLBhostname.domain*.

Si vous utilisez une configuration de Workspace ONE Access en cluster, notez que Lifecycle Manager ne peut pas mettre à jour le certificat d'équilibrage de charge, vous devez donc le mettre à jour manuellement. En outre, si vous devez réenregistrer des produits ou des services externes à Lifecycle Manager, il s'agit d'un processus manuel.

Ce chapitre contient les rubriques suivantes :

- [Configurer la mutualisation entre plusieurs organisations pour vRealize Automation](#)
- [Connexion aux locataires et ajout d'utilisateurs dans vRealize Automation](#)
- [Utilisation de vRealize Orchestrator avec des déploiements vRealize Automation à plusieurs organisations](#)

Configurer la mutualisation entre plusieurs organisations pour vRealize Automation

Vous pouvez configurer la mutualisation entre plusieurs organisations pour vRealize Automation à l'aide de vRealize Suite Lifecycle Manager.

Vous trouverez ci-dessous une description détaillée de la procédure de configuration de l'architecture mutualisée de vRealize Automation, notamment la configuration de DNS et des certificats. Elle porte principalement sur un déploiement à nœud unique, mais inclut des notes sur une configuration en cluster.

Reportez-vous à la section <https://vmwarelab.org/2020/04/14/vrealize-automation-8-1-multi-tenancy-setup-with-vrealize-suite-lifecycle-manager-8-1/> pour plus d'informations et une démonstration vidéo d'une configuration vRealize Automation à plusieurs organisations.

Conditions préalables

- Installez et configurez Workspace ONE Access version 3.3.2.
- Installez et configurez vRealize Suite Lifecycle Manager version 8.1.

Procédure

- 1 Créez les enregistrements DNS de type A et CNAME requis.
 - Pour votre locataire principal et chaque sous-locataire, vous devez créer et appliquer un certificat SAN.
 - Pour les déploiements à un seul nœud, le nom de domaine complet de vRealize Automation pointe vers le dispositif vRealize Automation et le nom de domaine complet de Workspace ONE Access pointe vers le dispositif Workspace ONE Access.

- Pour les déploiements en cluster, les noms de domaine complets basés sur des locataires Workspace ONE Access et vRealize Automation doivent pointer vers leurs équilibres de charge respectifs. Workspace ONE Access est configuré avec une terminaison SSL, de sorte que le certificat est appliqué à la fois au cluster Workspace ONE Access et à l'équilibrage de charge. L'équilibrage de charge vRealize Automation utilise le relais SSL, de sorte que le certificat est appliqué uniquement sur le cluster vRealize Automation.

Pour obtenir des informations détaillées, consultez [Gestion des certificats et de la configuration DNS dans des déploiements dans plusieurs organisations à nœud unique](#) et [Gestion de la configuration des certificats et de DNS sous des déploiements vRealize Automation en cluster](#).

- 2 Créez ou importez les certificats multi-domaines (SAN) requis pour Workspace ONE 3.3.2 et vRA 8.1.

Vous pouvez créer des certificats dans Lifecycle Manager à l'aide du service Locker qui vous permet de créer des licences de certificats et des mots de passe. Vous pouvez également utiliser un serveur d'autorité de certification ou un autre mécanisme pour générer des certificats.

Si vous avez besoin d'ajouter ou de créer des locataires supplémentaires, vous devez recréer et appliquer vos locataires vRealize Automation et Workspace ONE Access.

Après avoir créé vos certificats, vous pouvez les appliquer dans Lifecycle Manager à l'aide de la fonctionnalité des opérations de cycle de vie. Vous devez sélectionner l'environnement et le produit, puis l'option Remplacer le certificat dans le menu à droite. Ensuite, vous pouvez sélectionner le produit. Lorsque vous remplacez un certificat, vous devez réapprouver tous les produits associés dans votre environnement.

Vous devez attendre que le certificat soit appliqué et que tous les services redémarrent avant de passer à l'étape suivante.

Pour obtenir des informations détaillées, consultez [Gestion des certificats et de la configuration DNS dans des déploiements dans plusieurs organisations à nœud unique](#) et [Gestion de la configuration des certificats et de DNS sous des déploiements vRealize Automation en cluster](#).

- 3 Appliquez le certificat Workspace ONE SAN sur l'instance de Workspace ONE Access ou le cluster.
- 4 Dans vRealize Suite Lifecycle Manager 8.1, exécutez l'assistant Activer le locataire pour activer l'architecture mutualisée et créer un alias pour le locataire principal par défaut.

L'activation du locataire nécessite la création d'un alias pour le locataire principal de l'organisation du fournisseur ou le locataire par défaut. Une fois que vous avez activé le locataire, vous pouvez accéder à Workspace ONE Access via le nom de domaine complet du locataire principal.

Par exemple, si le nom de domaine complet existant de Workspace ONE Access est `idm.example.local` et que vous créez un alias de locataire par défaut, une fois que le locataire est activé, le nom de domaine complet de Workspace ONE Access devient `default-tenant.example.local`, et tous les clients communiquant avec Workspace ONE Access peuvent désormais communiquer via `default-tenant.example.local`.

- 5 Appliquez les certificats vRealize Automation SAN sur l'instance de vRealize Automation ou le cluster.

Vous pouvez appliquer des certificats SAN via le service des opérations de cycle de vie de Lifecycle Manager. Vous devez afficher les détails de l'environnement, puis sélectionner Remplacer les certificats dans le menu de droite. Vous devez attendre la fin de la tâche de remplacement des certificats avant d'ajouter des locataires. Dans le cadre du remplacement des certificats, les services vRealize Automation vont redémarrer.

- 6 Dans Lifecycle Manager, exécutez l'assistant Ajouter des locataires pour configurer les locataires souhaités.

Vous ajoutez des locataires à l'aide de la page Gestion des locataires de Lifecycle Manager située sous Gestion des identités et des locataires. Vous pouvez uniquement ajouter des locataires pour lesquels vous avez précédemment configuré des certificats et des paramètres DNS.

Lors de la création d'un locataire, vous devez désigner un administrateur de locataire et vous pouvez sélectionner les connexions Active Directory pour ce locataire. Les connexions disponibles sont basées sur celles configurées dans votre locataire par défaut ou principal. Vous devez également sélectionner le produit ou une instance du produit auquel le locataire sera associé.

Étape suivante

Après avoir créé des locataires, vous pouvez utiliser la page Gestion des locataires de Lifecycle Manager située sous Gestion des identités et des locataires pour modifier ou ajouter des administrateurs de locataires, ajouter des annuaires Active Directory au locataire et modifier les associations de produits pour le locataire.

Vous pouvez également vous connecter à votre instance de Workspace ONE Access pour afficher et valider la configuration de votre locataire.

Gestion des certificats et de la configuration DNS dans des déploiements dans plusieurs organisations à nœud unique

Les configurations de vRealize Automation avec mutualisation entre plusieurs organisations reposent sur une configuration coordonnée entre plusieurs produits. Vous devez donc vous assurer que les paramètres DNS et les certificats sont correctement configurés pour que votre configuration avec mutualisation entre plusieurs organisations fonctionne.

Cette configuration à plusieurs organisations suppose des déploiements à nœud unique pour les composants suivants :

- Lifecycle Manager
- Workspace ONE Access Identity Manager
- vRealize Automation

En outre, elle suppose de démarrer avec un locataire par défaut, qui est l'organisation de votre fournisseur, et de créer deux sous-locataires, appelés tenant-1 et tenant-2.

Vous pouvez créer et appliquer des certificats à l'aide du service Locker dans vRealize Suite Lifecycle Manager ou vous pouvez utiliser un autre mécanisme. Lifecycle Manager vous permet également de remplacer ou de réapprouver des certificats sur vRealize Automation ou Workspace ONE Access.

Conditions requises de DNS

Vous devez créer des enregistrements de type A principaux et des enregistrements de type CNAME pour les composants système, comme décrit ci-dessous.

- Créez des enregistrements de type A principaux pour chaque composant système et pour chacun des locataires que vous créez lorsque vous activez l'architecture mutualisée.
- Créez des enregistrements de type A à locataires multiples pour chacun des locataires que vous allez créer, ainsi que pour le locataire principal.
- Créez des enregistrements de type CNAME à locataires multiples pour chacun des locataires que vous allez créer, sans inclure le locataire principal.

Conditions requises des certificats pour un déploiement à locataires multiples à nœud unique

Vous devez créer deux certificats SAN (Subject Alternative Name), un premier pour Workspace ONE Access et un autre pour vRealize Automation.

- Le certificat vRealize Automation répertorie le nom d'hôte du serveur vRealize Automation et les noms des locataires que vous allez créer.
- Le certificat Workspace ONE Access répertorie le nom d'hôte du serveur Workspace ONE Access et les noms des locataires que vous créez.

- Si vous utilisez des noms SAN dédiés, les certificats doivent être mis à jour manuellement lorsque vous ajoutez ou supprimez des hôtes, ou lorsque vous modifiez un nom d'hôte. Vous devez également mettre à jour des entrées DNS pour les locataires. Pour simplifier la configuration, vous pouvez utiliser des caractères génériques pour les certificats Workspace ONE Access et vRealize Automation. Par exemple, *.example.com et *.vra.example.com.

Note vRealize Automation 8.x prend en charge les certificats génériques uniquement pour les noms DNS qui correspondent aux spécifications de la liste de suffixes publics sur <https://publicsuffix.org>. Par exemple, *.myorg.com est un nom valide alors que *.myorg.local ne l'est pas.

Notez que Lifecycle Manager ne crée pas de certificats distincts pour chaque locataire. Il crée plutôt un certificat unique avec chaque nom d'hôte de locataire répertorié. Pour les configurations de base, le CNAME du locataire utilise le format suivant : *tenantname.vrahostname.domain*. Pour les configurations à haute disponibilité, le nom utilise le format suivant : *tenantname.vraLBhostname.domain*.

Résumé

Le tableau suivant récapitule les conditions requises de DNS et de certificat pour un déploiement Workspace ONE Access et vRealize Automation à nœud unique.

Conditions requises de DNS	Conditions requises des certificats SAN
Main A Type Records lcm.example.local WorkspaceOne.example.local vra.example.local	Workspace One Certificate Nom de l'hôte : WorkspaceOne.example.local, default-tenant.example.local, tenant-1.vra.example.local, tenant-2.vra.example.local
Multi-tenancy A Type Records default-tenant.example.local tenant-1.example.local tenant-2.example.local	
Multi-Tenancy CNAME Type Records tenant-1.vra.example.local tenant-2.vra.example.local	vRealize Automation Certificate Nom de l'hôte : vra.example.local, tenant-1.vra.example.local, tenant-2.vra.example.local

Gestion de la configuration des certificats et de DNS sous des déploiements vRealize Automation en cluster

Vous devez coordonner la configuration des certificats et de DNS entre tous les composants applicables pour configurer un déploiement vRealize Automation en cluster à plusieurs organisations.

Dans une configuration en cluster classique, il y a trois dispositifs Workspace ONE Access et trois dispositifs vRealize Automation, ainsi qu'un dispositif Lifecycle Manager unique.

Cette configuration suppose des déploiements en cluster pour les composants suivants :

- Dispositifs Workspace ONE Access Identity Manager :
 - idm1.example.local
 - idm2.example.local
 - idm3.example.local
 - idm-lb.example.local
- Dispositifs vRealize Automation :
 - vra1.example.local
 - vra2.example.local
 - vra3.example.local
 - vra-lb.example.local
- Dispositif Lifecycle Manager

Conditions requises de DNS

Vous devez créer des enregistrements de type A principaux pour chaque composant et pour chacun des locataires que vous créez lorsque vous activez l'architecture mutualisée. En outre, vous devez créer des enregistrements de type CNAME à locataires multiples pour chacun des locataires que vous allez créer, sans inclure le locataire principal. Enfin, vous devez également créer des enregistrements de type A principaux pour les équilibres de charge Workspace ONE Access et vRealize Automation.

- Créez des enregistrements de type A pour les trois dispositifs Workspace ONE Access et pour les dispositifs vRealize Automation qui pointent vers leurs noms de domaine complets respectifs.
- En outre, créez des enregistrements de type A pour l'équilibrage de charge Workspace ONE Access et l'équilibrage de charge vRealize Automation qui pointent vers leurs noms de domaine complets respectifs.
- Créez des enregistrements de type A à locataires multiples pour le locataire par défaut et pour les locataires tenant-1 et tenant-2 qui pointent vers l'adresse IP de l'équilibrage de charge Workspace ONE Access.
- Créez des enregistrements CNAME pour les locataires tenant-1 et tenant-2 qui pointent vers l'adresse IP de l'équilibrage de charge vRealize Automation.

Conditions requises des certificats SAN (Subject Alternative Name)

Vous devez créer deux certificats Workspace ONE Access, un premier qui s'applique aux dispositifs de cluster, un autre qui s'applique à l'équilibrage de charge. En outre, créez un certificat qui s'applique aux dispositifs vRealize Automation, aux locataires que vous créez (à l'exception du locataire par défaut) et à l'équilibrage de charge.

- Créez un certificat pour les dispositifs Workspace ONE Access qui répertorient les noms de domaine complets des dispositifs Workspace ONE Access, ainsi que le locataire par défaut et d'autres locataires que vous créez. Ce certificat doit inclure les adresses IP des dispositifs Workspace ONE Access.
- Nous vous recommandons de créer une terminaison SSL sur l'équilibrage de charge. Pour prendre en charge cette terminaison, créez un certificat pour l'équilibrage de charge Workspace ONE Access qui répertorie les noms de domaine complets de l'équilibrage de charge Workspace ONE Access ainsi que le locataire par défaut et tous les autres locataires que vous créez. Ce certificat doit inclure l'adresse IP de l'équilibrage de charge.
- Vous devez créer un certificat pour vRealize Automation qui répertorie les noms d'hôte des trois dispositifs vRealize Automation, ainsi que l'équilibrage de charge associé et les locataires que vous créez. En outre, il doit répertorier les adresses IP des trois dispositifs vRealize Automation.
- Pour simplifier la configuration, vous pouvez utiliser des caractères génériques pour les certificats Workspace ONE Access et vRealize Automation. Par exemple, *.example.com, *.vra.example.com et *.vra-lb.example.com.

Note vRealize Automation 8.x prend en charge les certificats génériques uniquement pour les noms DNS qui correspondent aux spécifications de la liste de suffixes publics sur <https://publicsuffix.org>. Par exemple, *.myorg.com est un nom valide alors que *.myorg.local ne l'est pas.

Si vous utilisez une configuration de Workspace ONE Access en cluster, notez que Lifecycle Manager ne peut pas mettre à jour les certificats d'équilibrage de charge. Vous devez donc les mettre à jour manuellement. En outre, si vous devez réenregistrer des produits ou des services externes à Lifecycle Manager, il s'agit d'un processus manuel.

Résumé des entrées DNS et des certificats pour une configuration à plusieurs organisations en cluster

Le tableau suivant présente les conditions requises de DNS et de certificat pour un déploiement à plusieurs organisations en cluster de Workspace ONE Access et de vRealize Automation.

Conditions requises de DNS	Conditions requises des certificats SAN
Main A Type Records lcm.example.local WorkspaceOne-1.example.local WorkspaceOne-2.example.local WorkspaceOne-3.example.local vra.example-1.local vra.example-2.local vra.example-3.local	Workspace One Certificate Nom de l'hôte : WorkspaceOne.example.local, default-tenant.example.local, tenant-1.example.local, tenant-2.example.local
Multi-Tenancy A Type Records default-tenant.example.local tenant-1.vra.example.local tenant-2.vra.example.local	Workspace One LB Certificate (LB Terminated) Nom de l'hôte : WorkSpaceOne-lb.example.local, default-tenant.example.local, vra.example.local, tenant-1.example.local, tenant-2.example.local
Multi-Tenancy CNAME Type Records tenant-1.vra-lb.example.local - vra-lb.example.local tenant-2.vra-lb.example.local - vra.lb.exmple.local	vRealize Automation Certificate Nom de l'hôte : vra-1.example.local, vra-2.example.local, vra-3.example.local, vra- lb.example.local, tenant-1.example.local, tenant-2.example.local Aucun certificat n'est requis sur l'équilibrage de charge de vRealize Automation, car il utilise le relais SSL.

Connexion aux locataires et ajout d'utilisateurs dans vRealize Automation

Une fois que vous avez créé des locataires pour vRealize Automation dans Lifecycle Manager, vous pouvez vous connecter à Workspace ONE Access pour afficher vos locataires et ajouter des utilisateurs.

Vous pouvez afficher les locataires créés pour un déploiement vRealize Automation en vous connectant à l'instance associée de Workspace ONE Access. L'URL à utiliser est `https://default-tenant.name.domainname.local` ou, pour un déploiement non mis en cluster, `https://idm.domainname.local` qui vous redirigera vers l'URL Workspace ONE Access du locataire par défaut.

Vous pouvez valider des locataires spécifiques dans Workspace ONE Access à l'aide de l'URL suivante : `https://tenant-1.domainname.local`. Cette URL ouvre une page qui affiche les utilisateurs du locataire spécifié. Vous pouvez cliquer sur **Ajouter un utilisateur** pour créer des utilisateurs supplémentaires ad hoc.

Les utilisateurs autorisés peuvent se connecter à l'organisation principale du fournisseur dans vRealize Automation à l'aide de `https://vra.domainname.local`. Cette vue donne accès à tous les services vRealize Automation associés.

Les utilisateurs autorisés peuvent se connecter aux locataires applicables dans vRealize Automation en utilisant `https://tenantname.vra.domainname.local`.

Pour plus d'informations sur la gestion des utilisateurs dans Workspace ONE Access, consultez <https://docs.vmware.com/fr/VMware-Workspace-ONE-Access/3.3/idm-administrator.pdf>

Ajout d'utilisateurs locaux

Vous pouvez ajouter des utilisateurs locaux à votre déploiement à l'aide de l'instance associée de Workspace ONE Access. Les utilisateurs locaux sont des utilisateurs qui ne sont pas stockés dans un fournisseur d'identité externe.

Utilisation de vRealize Orchestrator avec des déploiements vRealize Automation à plusieurs organisations

Vous pouvez utiliser vRealize Orchestrator avec les déploiements de locataires vRealize Automation dans plusieurs organisations.

Le locataire par défaut prend en charge l'intégration avec l'intégration intégrée de vRealize Orchestrator d'origine. vRealize Orchestrator est disponible préalablement configuré sur la page Intégrations. Les sous-locataires n'ont pas d'intégration vRealize Orchestrator préenregistrée. Ils disposent de plusieurs options pour ajouter l'intégration de vRealize Orchestrator.

- Ils peuvent ajouter une intégration à l'instance intégrée de vRealize Orchestrator en accédant à Configurer le fournisseur d'authentification dans vRealize Orchestrator et en se connectant à l'aide de l'adresse d'hôte du locataire vRealize Automation applicable. Ils peuvent ensuite sélectionner **Infrastructure > Connexions > Intégrations** et ajouter l'instance intégrée de vRO en tant qu'intégration.
- Ils peuvent ajouter une instance externe de vRealize Orchestrator qui utilise l'instance de vRealize Automation à plusieurs organisations en tant que fournisseur d'authentification.

Toute instance de vRealize Orchestrator qui utilise un déploiement vRealize Automation à plusieurs organisations en tant que fournisseur d'authentification peut être enregistrée sur l'un des locataires en créant une nouvelle intégration et en fournissant le nom de domaine complet de vRealize Orchestrator sans fournir d'informations d'identification.

Utilisation des journaux dans vRealize Automation

5

Vous pouvez utiliser l'utilitaire de ligne de commande `vracli` fourni pour créer et utiliser des journaux dans vRealize Automation.

Vous pouvez utiliser des journaux directement dans vRealize Automation ou vous pouvez transférer tous les journaux vers vRealize Log Insight.

Ce chapitre contient les rubriques suivantes :

- [Utilisation des journaux et des bundles de journaux dans vRealize Automation](#)
- [Configuration du transfert de journaux vers vRealize Log Insight](#)
- [Comment créer ou mettre à jour une intégration syslog dans vRealize Automation](#)

Utilisation des journaux et des bundles de journaux dans vRealize Automation

Vous pouvez créer et utiliser des journaux vRealize Automation et des bundles de journaux dans vRealize Automation.

Vous pouvez également transférer automatiquement les journaux vers vRealize Log Insight. Pour plus d'informations sur le transfert des journaux vers vRealize Log Insight, reportez-vous à [Configuration du transfert de journaux vers vRealize Log Insight](#).

Vous pouvez obtenir des informations sur l'utilisation de l'utilitaire de ligne de commande `vracli` en utilisant l'argument `--help` dans la ligne de commande `vracli`. Par exemple : `vracli log-bundle --help`

Commandes de bundles de journaux

Vous pouvez créer un bundle de journaux simple ou un journal agrégé (stockage à froid) de tous les services. Bien que les deux bundles de journaux contiennent tous les journaux de vos services, le bundle de stockage à froid contient une copie d'un flux agrégé des versions de sauvegarde des journaux de service, qui peut fournir une valeur de dépannage supplémentaire. L'agent de stockage à froid agrège constamment les journaux des services et les stocke sur le système de fichiers local. Un bundle de journaux simple contient généralement tout ce dont vous avez besoin pour le dépannage.

Vous pouvez également modifier la valeur de délai d'attente par défaut pour la collecte des journaux à partir de chaque nœud.

Dans un environnement en cluster, il vous suffit d'exécuter la commande `vracli log-bundle` sur un nœud.

- Afficher l'aide de la commande du bundle de journaux :

```
vracli log-bundle --help
```

- Créez un bundle de journaux simple.

```
vracli log-bundle
```

- Créer un bundle de journaux de stockage à froid :

```
vracli log-bundle --include-cold-storage
```

- Modifiez la valeur du délai d'expiration pour la collecte des journaux à partir de chaque nœud. Par exemple, si votre environnement contient des fichiers journaux volumineux, présente une mise en réseau lente ou une utilisation élevée du CPU, vous devrez peut-être définir le délai d'expiration sur une valeur supérieure à la valeur par défaut de 1 000 secondes.

```
vracli log-bundle --collector-timeout $CUSTOM_TIMEOUT_IN_SECONDS
```

Structures de bundles de journaux

Les services vRealize Automation sont déployés en conteneur dans des espaces Kubernetes. Le bundle de journaux généré est une archive `tar.xz` qui utilise un format de nom `log-bundle-{{TIMESTAMP}}.tar.xz`, où `TIMESTAMP` est un horodatage de la version en secondes. Un bundle de journaux normal contient des journaux de tous les nœuds de l'environnement. Si le bundle de journaux ne peut pas être généré pour une raison quelconque, un bundle de secours est créé à la place. Le bundle de secours contient les journaux du nœud actuel uniquement. Il existe de légères différences dans la structure des deux types de bundles de journaux.

- Bundles de journaux normaux

Les bundles de journaux normaux sont organisés dans les catégories suivantes :

- Journaux d'hôte et configuration

La configuration de chaque hôte et ses journaux spécifiques sont collectés dans un répertoire unique par nœud de cluster (hôte). Le nom du répertoire correspond au nom d'hôte du nœud. Le contenu du répertoire correspond au système de fichiers de l'hôte. Le nombre de répertoires correspond au nombre de nœuds de cluster.

Les journaux de stockage à froid sont situés dans un journal JSON structuré en tant que `/hostname/services-logs/all/aggregated.log`.

- Journaux d'espace

Les services sont déployés en conteneur dans des espaces Kubernetes. Les journaux de service se trouvent dans le répertoire `pods`, qui contient un seul répertoire par espace de noms avec un nom de fichier qui correspond au nom de l'espace de noms. Il y a généralement une instance de chaque espace par nœud de cluster. Le répertoire de l'espace contient un fichier journal pour chaque application de conteneur.

Par exemple, les journaux du centre de contrôle de vRealize Orchestrator résident dans un fichier `vco-controlcenter-app.log` dans chacun des répertoires `/pods/prelude/vco-app-hash/`.

- Fichier d'environnement

Le fichier d'environnement contient des informations sur l'utilisation actuelle des ressources par nœud et par espace. Il contient également des informations sur le cluster et des descriptions pour toutes les entités Kubernetes disponibles.

- Bundles de journaux de secours

Si vous recevez un message d'erreur lors de l'attente de la fin de la commande `vrac li`, un bundle de secours est généré. Si vous recevez cette erreur, vous devez exécuter la commande `vrac li log-bundle` sur chaque hôte ou nœud du cluster pour collecter autant d'informations que possible.

- Journaux de conteneur de secours

Les journaux de secours se trouvent dans le répertoire `/fallback-containers`. Vous pouvez identifier le conteneur dans lequel l'espace a généré les journaux en examinant le nom du fichier journal :

```
pod-name-some-hash-container-name-other-hash.log
```

- Stockage à froid de secours

Si vous collectez des journaux de stockage à froid avec le bundle, les journaux de secours de l'hôte actuel se trouvent dans le répertoire `/fallback-cold-storage`.

Configuration du transfert de journaux vers vRealize Log Insight

Vous pouvez transférer des journaux depuis vRealize Automation vers vRealize Log Insight pour bénéficier d'une analyse de journaux et d'une génération de rapports plus robustes.

vRealize Automation est fourni avec un agent de journalisation [fluentd-based](#). Cet agent collecte et stocke les journaux de sorte qu'ils puissent être inclus dans un bundle de journaux et examinés ultérieurement. Vous pouvez configurer l'agent pour qu'il transfère une copie des journaux vers un serveur vRealize Log Insight à l'aide de l'API de vRealize Log Insight. L'API fournie permet à d'autres programmes de communiquer avec vRealize Log Insight.

Pour plus d'informations sur vRealize Log Insight, y compris la documentation de l'API de vRealize Log Insight, consultez la [documentation de vRealize Log Insight](#) et également la page `/api/v1/events/ingest/{agentId}`.

Configurez l'agent de journalisation pour qu'il transfère automatiquement et continuellement les journaux vRealize Automation vers vRealize Log Insight à l'aide de l'utilitaire de ligne de commande `vracli` fourni.

Toutes les lignes de journal sont balisées avec un nom d'hôte et une balise d'environnement et peuvent être examinées dans vRealize Log Insight. Dans un environnement à haute disponibilité (HA), les journaux sont balisés avec des noms d'hôte différents, en fonction du nœud sur lequel ils ont été créés. La balise d'environnement peut être configurée avec l'option `--environment ENV` comme décrit ci-dessous dans la section *Configurer ou mettre à jour l'intégration de vRealize Log Insight*. Dans un environnement HA, la balise d'environnement a la même valeur pour toutes les lignes de journal, quel que soit le nœud sur lequel elle a été créée.

Vous pouvez obtenir des informations sur l'utilisation de l'utilitaire de ligne de commande `vracli` en utilisant l'argument `--help` dans la ligne de commande `vracli`. Par exemple : `vracli vrli --help`

Vérifier la configuration existante de vRealize Log Insight

Command

```
vracli vrli
```

Arguments

Il n'y a aucun argument de ligne de commande.

Output

La sortie de la configuration actuelle de l'intégration de vRealize Log Insight est au format JSON.

Exit codes

Les codes de sortie suivants sont possibles :

- 0 - L'intégration à vRealize Log Insight est configurée.
- 1 - Une exception s'est produite dans le cadre de l'exécution de la commande. Pour plus de détails, consultez le message d'erreur.
- 61 (ENODATA) - L'intégration à vRealize Log Insight n'est pas configurée. Pour plus de détails, consultez le message d'erreur.

Exemple – check integration configuration

```
$ vracli vrli
No vRLI integration configured

$ vracli vrli
{
  "agentId": "0",
  "environment": "prod",
  "host": "my-vrli.local",
```

```
"port": 443,
"scheme": "https",
"sslVerify": false
}
```

Note Vous pouvez définir un autre schéma (la valeur par défaut est https) et port (la valeur par défaut est 443) d'hôte à utiliser pour l'envoi des journaux, comme indiqué dans les exemples suivants :

```
vracli vrli set some-host
vracli vrli set some-host:9543
vracli vrli set http://some-host:9543
```

Le port 9543 est utilisé par l'API d'ingestion de vRealize Log Insight comme décrit dans la rubrique *Administration de vRealize Log Insight* de la section *Ports et interfaces externes* dans la [Documentation vRealize log Insight](#).

Configurer ou mettre à jour l'intégration de vRealize Log Insight

Command

```
vracli vrli set [options] FQDN_OR_URL
```

Arguments

Les arguments de ligne de commande suivants sont disponibles :

- FQDN_OR_URL - Nom de domaine complet ou adresse IP du serveur vRealize Log Insight qui doit être utilisé pour publier les journaux à l'aide de la configuration de l'API de vRealize Log Insight. Le port 443 et un schéma HTTPS sont utilisés par défaut. Si l'un de ces paramètres doit être modifié, vous pouvez utiliser une URL à la place.
- options
 - --agent-id SOME_ID - Définissez l'ID de l'agent de journalisation pour ce dispositif. La valeur par défaut est 0. Permet d'identifier l'agent de journalisation pour les journaux publiés vers vRealize Log Insight à l'aide de la configuration de l'API de vRealize Log Insight.
 - --environment ENV - Définissez un identifiant pour l'environnement actuel. Il sera disponible dans les journaux vRealize Log Insight en tant que balise pour chaque événement de ligne de journal. La valeur par défaut est prod.
 - --ca-file /path/to/server-ca.crt - Spécifiez un fichier contenant le certificat de l'autorité de certification (CA) qui a été utilisé pour signer le certificat de serveur vRealize Log Insight. Forcez l'agent de journalisation à approuver l'autorité de certification spécifiée et activez-la pour vérifier le certificat du serveur vRealize Log Insight. Le fichier peut contenir une chaîne de certificats complète, si nécessaire, pour vérifier le certificat. Dans le cas d'un certificat auto-signé, transmettez le certificat lui-même.

- `--ca-cert CA_CERT` - Spécifiez un fichier de la même manière que pour `--ca-file`, mais transmettez le certificat (chaîne) en ligne en tant que chaîne.
- `--insecure` - Désactivez la vérification SSL du certificat de serveur. Forcez l'agent de journalisation à accepter n'importe quel certificat SSL lors de la publication de journaux.

Output

Aucune sortie n'est attendue.

Exit codes

Les codes de sortie suivants sont possibles :

- 0 - La configuration a été mise à jour.
- 1 - Une exception s'est produite lors de l'exécution. Pour plus de détails, consultez le message d'erreur.

Exemples – Configure or update integration configuration

```
$ vracli vrli set my-vrli.local
$ vracli vrli set 10.20.30.40

$ vracli vrli set --ca-file /etc/ssl/certs/ca.crt 10.20.30.40

$ vracli vrli set --ca-cert "$(cat /etc/ssl/certs/ca.crt)" 10.20.30.40

$ vracli vrli set --insecure http://my-vrli.local:8080

$ vracli vrli set --agent-id my-vrli-agent my-vrli.local

$ vracli vrli set --environment staging my-vrli.local
```

Effacer l'intégration de vRealize Log Insight

Command

```
vracli vrli unset
```

Arguments

Il n'y a aucun argument de ligne de commande.

Output

La sortie de la confirmation est au format texte simple.

Exit codes

Les codes de sortie suivants sont possibles :

- 0 - La configuration a été effacée ou aucune configuration n'existait.
- 1 - Une exception s'est produite lors de l'exécution. Pour plus de détails, consultez le message d'erreur.

Exemples – Clear integration

```
$ vracli vrli unset  
Clearing vRLI integration configuration  
  
$ vracli vrli unset  
No vRLI integration configured
```

Comment créer ou mettre à jour une intégration syslog dans vRealize Automation

Vous pouvez configurer vRealize Automation pour envoyer vos informations de journalisation à des serveurs syslog distants.

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

L'intégration syslog distante de vRealize Automation prend en charge les types de connexion suivants :

- Sur UDP.
- Sur TCP sans TLS.

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

- Sur TCP avec TLS.

Pour plus d'informations sur la configuration de l'intégration de journalisation avec vRealize Log Insight, reportez-vous à [Configuration du transfert de journaux vers vRealize Log Insight](#).

Conditions préalables

Configurez un ou plusieurs serveurs syslog distants.

Procédure

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

- 2 Pour créer une intégration à un serveur Syslog, exécutez la commande `vracli remote-syslog set`.

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

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

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

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

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

Étape suivante

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

Comment supprimer une intégration syslog pour la journalisation dans vRealize Automation

Vous pouvez supprimer des intégrations syslog de votre dispositif vRealize Automation en exécutant la commande `vracli remote-syslog unset`.

Conditions préalables

Créez une ou plusieurs intégrations syslog dans le dispositif vRealize Automation. Voir [Comment créer ou mettre à jour une intégration syslog dans vRealize Automation](#).

Procédure

- 1 Connectez-vous à la ligne de commande du dispositif vRealize Automation en tant qu'utilisateur **racine**.
- 2 Supprimez les intégrations syslog du dispositif vRealize Automation à l'aide de l'une des méthodes suivantes :
 - Pour supprimer une intégration syslog spécifique, exécutez la commande `vracli remote-syslog unset -id Integration_name`.

- Pour supprimer toutes les intégrations syslog sur le dispositif vRealize Automation, exécutez la commande `vracli remote-syslog unset` sans l'indicateur `-id`.

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

Participation au Programme d'amélioration du produit pour vRealize Automation

6

Ce produit fait partie du programme d'amélioration du produit de VMware (CEIP). Ce programme fournit à VMware des informations lui permettant d'améliorer ses produits et services, de corriger certains problèmes et de vous informer sur la meilleure façon de déployer et d'utiliser ses produits.

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>.

Ce chapitre contient les rubriques suivantes :

- [Rejoindre ou quitter le Programme d'amélioration du produit pour vRealize Automation](#)
- [Configuration de l'heure de collecte des données pour le Programme d'amélioration du produit de vRealize Automation](#)

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

Vous pouvez rejoindre ou quitter le programme d'amélioration du produit (CEIP) depuis l'interface de ligne de commande du dispositif vRealize Automation.

Vous pouvez rejoindre le programme CEIP lorsque vous installez vRealize Automation et avec vRealize Lifecycle Manager (LCM). Vous pouvez également rejoindre ou quitter le programme à l'aide des options de ligne de commande après l'installation.

Pour rejoindre le programme d'amélioration du produit à l'aide des options de ligne de commande :

- 1 Connectez-vous à l'interface de ligne de commande du dispositif vRealize Automation en tant qu'utilisateur **racine**.
- 2 Exécutez la commande `vracli ceip on`.
- 3 Vérifiez les informations du programme d'amélioration du produit et exécutez la commande `vracli ceip on --acknowledge-ceip`.
- 4 Pour redémarrer les services vRealize Automation, exécutez la commande `/opt/scripts/deploy.sh`.

Pour quitter le programme d'amélioration du produit à l'aide des options de ligne de commande :

- 1 Connectez-vous à l'interface de ligne de commande du dispositif vRealize Automation en tant qu'utilisateur **racine**.
- 2 Exécutez la commande `vracli ceip off`.
- 3 Pour redémarrer les services vRealize Automation, exécutez la commande `/opt/scripts/deploy.sh`.

Configuration de l'heure de collecte des données pour le Programme d'amélioration du produit de vRealize Automation

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

Procédure

- 1 Connectez-vous à la ligne de commande du dispositif vRealize Automation en tant qu'utilisateur **racine**.
- 2 Ouvrez le fichier suivant dans un éditeur de texte.
`/etc/telemetry/telemetry-collector-vami.properties`
- 3 Modifiez les propriétés pour le jour de la semaine (dow) et l'heure du jour (hod).

Propriété	Description
<code>frequency.dow=<day-of-week></code>	Jour de la collecte de données.
<code>frequency.hod=<hour-of-day></code>	Heure locale du jour de collecte des données. Les valeurs possibles vont de 0 à 23.

- 4 Enregistrez et fermez `telemetry-collector-vami.properties`.
- 5 Appliquez les paramètres en entrant la commande suivante.

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

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