Administration de vRealize Automation

Octobre 2022
vRealize Automation 8.5

vmware®

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

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

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

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

Table des matières

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 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
■ Propriétaire d'organisation ■ Membre d'organisation	■ 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 vRealize Suite Lifecycle Manager et de Workspace ONE Access, reportez-vous aux sections suivantes.

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
- Activer la bannière Avis et consentement du Département de la Défense américain

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

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

Rôle	Description
Administrateur de Cloud Assembly	Utilisateur qui dispose d'un accès en lecture et en écriture à l'intégralité de l'interface utilisateur et des ressources d'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 Cloud Assembly, l'administrateur ajoute des utilisateurs aux projets en tant que membres, administrateurs ou observateurs du projet. L'administrateur peut également ajouter un administrateur de projet.
Observateur de Cloud Assembly	Utilisateur disposant d'un accès en lecture aux informations, mais qui ne peut pas créer, mettre à jour ou supprimer des valeurs. Ce rôle est en lecture seule dans tous les projets. Les utilisateurs qui disposent du rôle d'observateur peuvent afficher toutes les informations qui sont disponibles pour l'administrateur. Il ne peut effectuer aucune action, sauf si vous leur accordez un rôle d'administrateur de projet ou de membre du projet. Si l'utilisateur est affilié à un projet, il dispose des autorisations associées à ce rôle. Les autorisations de l'observateur de projet ne peuvent pas être étendues de la même manière que pour le rôle d'administrateur ou de membre.

Outre les rôles de service, Cloud Assembly a des rôles de projet. Les projets sont disponibles dans tous les services.

Les rôles de projet sont définis dans 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 modèles de cloud.

- 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 modèles de cloud.

Tableau 2-2. Rôles de service et rôles de projet 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				
	Mettre à jour ou supprimer des valeurs du résumé du projet, du provisionnement, de Kubernetes, des intégrations et des configurations du projet de test.	Oui				
	Ajoutez des utilisateurs et des groupes, 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				

Tableau 2-2. Rôles de service et rôles de projet 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 zones de cloud	Oui	Oui			
	Afficher le tableau de bord Analyses de la zone de cloud	Oui	Oui			
	Afficher les alertes des zones de cloud	Oui	Oui			
Configurer - Zones Kubernetes	Créer, mettre à jour ou supprimer des zones Kubernetes	Oui				
	Afficher les 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 les mappages d'image	Oui	Oui			
Configurer - Profils réseau	Créer, mettre à jour ou supprimer des profils réseau	Oui				
	Afficher les profils réseau d'image	Oui	Oui			

Tableau 2-2. Rôles de service et rôles de projet 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
Configurer - Profils de stockage	Créer, mettre à jour ou supprimer des profils de stockage	Oui				
	Afficher les profils de stockage d'image	Oui	Oui			
Configurer - fiches de tarification	Créer, mettre à jour ou supprimer des fiches de tarification	Oui				
	Afficher les fiches 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				
	Afficher les ressources réseau découvertes	Oui	Oui			

Tableau 2-2. Rôles de service et rôles de projet 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
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				
	Afficher les clusters et les espaces de noms Kubernetes	Oui	Oui	Oui. Vos projets	Oui. Vos projets	Oui. Vos projets

Tableau 2-2. Rôles de service et rôles de projet 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
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 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 modèles de cloud téléchargés dans l'onglet Conception	Oui		Oui. En cas d'association à vos projets.	Oui. En cas d'association à vos projets.	
Marketplace - Modèles de cloud	Télécharger un modèle de cloud	Oui				
	Afficher les modèles de cloud	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 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 modèles de cloud	Oui	Oui	Oui. Vos projets	Oui. Vos projets	Oui. Vos projets
Modèles de cloud	Créer, mettre à jour et supprimer des modèles de cloud	Oui		Oui. Vos projets	Oui. Vos projets	
	Afficher les modèles de cloud	Oui	Oui	Oui. Vos projets	Oui. Vos projets	Oui. Vos projets
	Télécharger des modèles de cloud	Oui	Oui	Oui. Vos projets	Oui. Vos projets	Oui. Vos projets

Tableau 2-2. Rôles de service et rôles de projet 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
	Charger des modèles de cloud	Oui		Oui. Vos projets	Oui. Vos projets	
	Déployer des modèles de cloud	Oui		Oui. Vos projets	Oui. Vos projets	
	Gérer la version et restaurer des modèles de cloud	Oui		Oui. Vos projets	Oui. Vos projets	
	Publier les modèles de cloud dans le catalogue	Oui		Oui. Vos projets	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

Tableau 2-2. Rôles de service et rôles de projet 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 déploiements, y compris les détails du déploiement, l'historique du déploiement, le prix, la surveillance, les alertes, l'optimisation et les informations de dépannage	Oui	Oui	Oui. Vos projets	Oui. Vos projets	Oui. Vos projets
	Gérer des alertes	Oui		Oui. Votre projet	Oui. votre projet	
	Exécuter les actions du jour 2 sur les déploiements en fonction des stratégies	Oui		Oui. Vos projets	Oui. Vos projets	
Alertes						
	Voir et ouvrir l'onglet Alertes	Oui	Oui	Oui	Oui	Oui
	Gérer des alertes	Oui		Oui. Vos projets	Oui. Vos projets	
	Afficher les alertes	Oui	Oui	Oui. Vos projets	Oui. Vos projets	Oui. Vos projets

Rôles de service Service Broker

Les rôles de service Service Broker déterminent ce que vous pouvez voir et faire dans 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 Service Broker. Dans un projet Service Broker, l'administrateur ajoute des utilisateurs aux projets en tant que membres, administrateurs ou observateurs du projet. L'administrateur peut également ajouter un administrateur de projet.
Observateur de Service Broker	Utilisateur disposant d'un accès en lecture aux informations, mais qui ne peut pas créer, mettre à jour ou supprimer des valeurs. Les utilisateurs qui disposent du rôle d'observateur peuvent afficher toutes les informations qui sont disponibles pour l'administrateur. Il ne peut effectuer aucune action, sauf si vous leur accordez un rôle d'administrateur de projet ou de membre du projet. Si l'utilisateur est affilié à un projet, il dispose des autorisations associées à ce rôle. Les autorisations de l'observateur de projet ne peuvent pas être étendues de la même manière que pour le rôle d'administrateur ou de membre.

Outre les rôles de service, Service Broker a des rôles de projet. Les projets sont disponibles dans tous les services.

Les rôles de projet sont définis dans 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 modèles de cloud.
- 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, du provisionnement, de Kubernetes, des intégrations et des configurations du projet de test.	Oui				
	Ajoutez des utilisateurs et des groupes, 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 les zones de cloud	Oui	Oui			
Configurer - Zones Kubernetes	Créer, mettre à jour ou supprimer des zones Kubernetes	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
	Afficher les 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			
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				

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
	Afficher le contenu partagé	Oui	Oui			
Contenu	Personnaliser un formulaire et configurer un élément	Oui				
	Afficher le contenu	Oui	Oui			
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

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
	Afficher les déploiements, y compris les détails du déploiement, l'historique du déploiement, le prix, la surveillance, les alertes, l'optimisation et les informations de dépannage	Oui	Oui	Oui. Vos projets	Oui. Vos projets	Oui. Vos projets
	Gérer des alertes	Oui		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	
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

Activer la bannière Avis et consentement du Département de la Défense américain

Pour certains clients du gouvernement des États-Unis, un administrateur doit configurer la bannière Avis et consentement standard du Département de la Défense américain dans Workspace ONE Access afin que les utilisateurs puissent accéder à vRealize Automation.

Le texte de la bannière Avis et consentement obligatoire standard du Département de la Défense américain est le suivant :

Vous accédez à un système d'information (SI) du gouvernement des États-Unis (GÉU) qui est fourni pour une utilisation autorisée par le gouvernement des États-Unis uniquement. En utilisant ce SI (qui inclut tous les périphériques attachés à ce SI), vous consentez aux conditions suivantes :

- Le GÉU intercepte et surveille régulièrement les communications sur ce SI pour des raisons incluant, sans s'y limiter, les tests de pénétration, la surveillance COMSEC, les opérations réseau et la défense, les manquements du personnel, l'application de la loi et les recherches de contre-espionnage.
- À tout moment, le GÉU peut inspecter et saisir les données stockées sur ce SI.
- Les communications utilisant ce SI ou les données stockées sur celui-ci ne sont pas privées. Elles font l'objet d'une surveillance, d'une interception et d'une recherche de routine, et peuvent être communiquées ou utilisées à des fins autorisées par le GÉU.

Les étapes suivantes décrivent comment configurer cette bannière dans Workspace ONE Access. Pour plus d'informations, consultez la documentation de la console d'administration de Workspace ONE Access.

Procédure

1. Connectez-vous à la console d'administration de Workspace ONE en tant qu'administrateur.
2. Dans la console VMware Identity Manager, cliquez sur l'onglet Gestion des identités et des accès.
3. Cliquez sur Configuration, puis sur l'onglet Connecteurs.
4. Cliquez sur le lien du nœud worker pour chaque connecteur que vous souhaitez configurer.
5. Cliquez sur l'onglet Adaptateurs d'authentification, puis cliquez sur `CertificateAuthAdapter`.
6. Cochez la case Activer le formulaire de consentement avant l'authentification.
7. Collez le texte de la bannière Avis et contentement obligatoire standard du Département de la Défense américain dans la zone Contenu du formulaire de consentement.
8. Enregistrez vos modifications.

Résultats

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

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

La manière recommandée d'arrêter et de démarrer les composants vRealize Automation consiste à utiliser les fonctionnalités Mettre hors tension et sous tension dans la section **Lifecycle Operations > Environnements** de vRealize Suite Lifecycle Manager. Les procédures suivantes décrivent les méthodes manuelles d'arrêt et de démarrage des composants vRealize Automation dans le cas où vRealize Suite Lifecycle Manager n'est pas disponible pour une raison quelconque.

Arrêter vRealize Automation

Pour préserver l'intégrité des données, arrêtez les services vRealize Automation avant de mettre hors tension les dispositifs virtuels. À l'aide de SSH ou de VMRC, vous pouvez arrêter ou démarrer tous les nœuds à partir de n'importe quel dispositif individuel.

Note Si possible, évitez d'utiliser la commande `vracli reset vidm`. Cette commande réinitialise toutes les configurations de Workspace ONE Access et rompt l'association entre les utilisateurs et les ressources provisionées.

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 équilibrages 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 :

```
kubectl -n prelude get pods
```

Montée en charge d'un nœud à trois nœuds pour un déploiement vRealize Automation

Si vous en avez besoin, vous pouvez effectuer une montée en charge pour un déploiement vRealize Automation d'un nœud à trois nœuds.

Vous devez utiliser les fonctionnalités de vRealize Suite Lifecycle Manager pour effectuer certaines étapes de cette procédure. 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.

Si vous utilisez un déploiement en cluster à trois nœuds, vRealize Automation peut généralement supporter la panne d'un nœud et continuer à fonctionner. La panne de deux nœuds dans un cluster à trois nœuds rend vRealize Automation non fonctionnel.

Conditions préalables

Cette procédure part du principe que vous disposez déjà d'un déploiement vRealize Automation à un nœud opérationnel.

Procédure

1 Arrêtez tous les dispositifs vRealize Automation.

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
```

Vous pouvez maintenant arrêter les dispositifs vRealize Automation.

2 Prenez un snapshot de déploiement.

Utilisez l'option Créer un snapshot dans le menu **Opérations de cycle de vie > Environnements > vRA > Afficher les détails** de vRealize Suite Lifecycle Manager.

Note Les snapshots en ligne pris sans arrêter les nœuds vRealize Automation sont pris en charge à partir de la version 8.0.1. Pour les environnements vRealize Automation 8.0, vous devez d'abord arrêter les nœuds vRealize Automation.

3 Mettez sous tension le dispositif vRealize Automation et activez tous les conteneurs.

4 L'utilisation de la fonctionnalité Locker située sous **LCM > Locker > Certificats** dans vRealize Suite Lifecycle Manager, génère ou importe des certificats vRealize Automation pour tous les composants, y compris pour les noms de domaine complets du nœud vRealize Suite Lifecycle Manageret le nom de domaine complet de l'équilibrage de charge vRealize Automation.

Ajoutez les noms des trois dispositifs dans les autres noms de l’objet.

5 Importez le nouveau certificat dans vRealize Suite Lifecycle Manager.

6 Remplacez le certificat vRealize Suite Lifecycle Manager existant par celui généré à l'étape précédente à l'aide de l'option Remplacer le certificat de LCM disponible sous **Opérations de cycle de vie > Environnements > vRA > Afficher les détails**.

7 Effectuez la montée en charge à trois nœuds de vRealize Automation à l'aide de la sélection Ajouter des composants dans **LCM > Opérations de cycle de vie > Environnements > vRA > Afficher les détails**.

Résultats

Vous avez effectué une montée en charge à trois nœuds du déploiement vRealize Automation.

Configurer une règle d'anti-affinité et un groupe de machines virtuelles pour une instance de Workspace ONE Access en cluster

Si votre environnement vRealize Automation utilise une instance de Workspace ONE Access en cluster, créez une règle d'anti-affinité et un cluster de machine pour garantir un workflow vSphere High Availability approprié.

Pour protéger les nœuds Workspace ONE Access en cluster contre une panne au niveau de l'hôte, configurez une règle d'anti-affinité pour exécuter les machines virtuelles qui existent sur des hôtes différents dans le cluster de gestion vSphere par défaut. Après avoir créé une règle d'anti-affinité configurez un groupe de machines virtuelles pour définir l'ordre de démarrage de machine souhaité. Vous pouvez vous assurer que vSphere High Availability met sous tension les nœuds Workspace ONE Access en cluster dans le bon ordre pour votre environnement en utilisant un ordre de démarrage de machine défini.

Pour plus d'informations sur la configuration de règles d'anti-affinité et d'un groupe de machines virtuelles, reportez-vous à la section Configurer une règle d'anti-affinité et un groupe de machines virtuelles pour l'instance de Workspace ONE Access en cluster dans la documentation du produit VMware Cloud Foundation.

Considérations relatives aux règles d'affinité lors de la mise à niveau d'une version de vRealize Automation vers une autre

vRealize Suite Lifecycle Manager ne prend pas en charge les règles d’anti-affinité pour vRealize Automation 8.x. Étant donné que vRealize Suite Lifecycle Manager est utilisé par vRealize Easy Installer pendant la mise à niveau de vRealize Automation et qu’il n’existe pas d’ordre spécifique de mise hors tension et sous tension des nœuds vRealize Automation pendant la mise à niveau, des problèmes peuvent se produire si l’ordre utilisé est en conflit avec les règles d’affinité qui définissent l’ordre dans lequel les machines sont mises hors tension et sous tension. Lorsque vous utilisez vRealize Suite Lifecycle Manager ou vRealize Easy Installer pour effectuer une mise à niveau d'une version de vRealize Automation vers une autre, désactivez les règles d'affinité avant de démarrer la mise à niveau.

Pour plus d'informations sur la mise à niveau d'une version de vRealize Automation vers une autre, reportez-vous à la section Installation de vRealize Automation avec vRealize Easy Installer dans la documentation du produit vRealize Automation.

Remplacement d'un nœud de dispositif vRealize Automation

Lorsqu'un dispositif vRealize Automation dans une configuration à plusieurs nœuds et à haute disponibilité (HA) échoue, vous pouvez avoir besoin de remplacer le nœud défectueux.

Attention Avant de poursuivre, VMware vous recommande de contacter le support technique afin de résoudre le problème lié à HA et de vérifier que le problème est isolé sur un nœud.

Si le support technique détermine que vous devez remplacer le nœud, prenez les mesures suivantes.

1 Dans vCenter, prenez des snapshots de sauvegarde de chaque dispositif dans la configuration HA.

   Dans les snapshots de sauvegarde, n'incluez pas la mémoire de machine virtuelle.

2 Arrêter le nœud défectueux.

3 Notez le numéro de build du logiciel vRealize Automation sur le nœud défectueux et les paramètres réseau.

   Notez le nom de domaine complet, l'adresse IP, la passerelle, les serveurs DNS et particulièrement l'adresse MAC. Ensuite, attribuez les mêmes valeurs au nœud de remplacement.

4 Le nœud de base de données principal doit être l'un des nœuds sains. Procédez comme suit :

   a Connectez-vous en tant qu'utilisateur racine à la ligne de commande d'un nœud sain.

   b Recherchez le nom du nœud de base de données principal en exécutant la commande suivante.

   ```
   vracli status | grep primary -B 1
   ```

   Le résultat doit être similaire à cet exemple, où postgres-1 est le nœud de base de données principal.

   ```
   "Conninfo":
   "host=postgres-1.postgres.prelude.svc.cluster.local
   dbname=repmgr-db user=repmgr-db passfile=/scratch/repmgr-db.cred
   connect_timeout=10",
   "Role": "primary",
   ```

   c Vérifiez que le nœud de base de données principal est sain en exécutant la commande suivante.

   ```
   kubectl -n prelude get pods -o wide | grep postgres
   ```

   Le résultat doit être semblable à cet exemple, où postgres-1 figure dans la liste comme étant en cours d'exécution et sain.

   ```
   postgres-1 1/1 Running 0 39h 12.123.2.14 vc-vm-224-84.company.com <none> <none>
   postgres-2 1/1 Running 0 39h 12.123.1.14 vc-vm-224-85.company.com <none> <none>
   ```

   Important Si le nœud principal de la base de données est défectueux, contactez le support technique au lieu de poursuivre.

5 À partir de la ligne de commande racine du nœud sain, supprimez le nœud défectueux.

   ```
   vracli cluster remove faulty-node-FQDN
   ```

6 Utilisez vCenter pour déployer un nouveau nœud vRealize Automation de remplacement.

Déployez le même numéro de build du logiciel vRealize Automation et appliquez les paramètres réseau à partir du nœud défectueux. Incluez le nom de domaine complet, l'adresse IP, la passerelle, les serveurs DNS et particulièrement l'adresse MAC que vous avez notés précédemment.

7 Mettez sous tension le nœud de remplacement.

8 Connectez-vous en tant qu'utilisateur racine à la ligne de commande du nœud de remplacement.

9 Vérifiez que la séquence de démarrage initiale s'est terminée en exécutant la commande suivante.

```
vracli status first-boot
```

Recherchez un message `First boot complete`.

10 À partir du nœud de remplacement, joignez le cluster vRealize Automation.

```
vracli cluster join primary-DB-node-FQDN
```

11 Connectez-vous en tant qu'utilisateur racine à la ligne de commande du nœud de base de données principal.

12 Déployez le cluster réparé en exécutant le script suivant.

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

Augmenter l'espace disque du dispositif vRealize Automation

Vous devrez peut-être augmenter l'espace disque du dispositif vRealize Automation à des fins telles que le stockage des fichiers journaux.

Procédure

1 Utilisez vSphere pour développer le VMDK sur le dispositif vRealize Automation.

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

3 Depuis l'invite de commande, exécutez la commande vRealize Automation suivante :

```
vracli disk-mgr resize
```

Si le redimensionnement de vRealize Automation échoue, consultez l'article 79925 de la base de connaissances.

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. Exécutez la commande suivante.

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

3. Vérifiez que les nouveaux serveurs DNS ont été correctement appliqués à tous les nœuds vRealize Automation à l'aide de la commande `vracli network dns status`.
4. Exécutez l'ensemble de commandes suivant pour arrêter les services vRealize Automation sur tous les nœuds du cluster.

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

5. Redémarrez les nœuds vRealize Automation et attendez qu'ils démarrent complètement.
6. Connectez-vous à chaque nœud de vRealize Automation avec SSH et vérifiez que les nouveaux serveurs DNS sont répertoriés dans `/etc/resolve.conf`.
7. 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	Cette configuration peut être utilisée 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. 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. **Note** Si votre déploiement vRealize Automation migre vers un hôte ESXi qui n'est pas synchronisé avec un serveur NTP, vous pouvez subir un décalage de l'horloge.
systemd	Cette configuration utilise le démon systemd-timesyncd pour synchroniser les horloges de votre déploiement vRealize Automation. **Note** Par défaut, le démon systemd-timesyncd 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.

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

   Vous pouvez également réinitialiser la configuration NTP à l'état par défaut en exécutant la commande `vracli ntp reset`.

3 Activez NTP avec systemd.

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

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

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

Résultats

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

Étape suivante

La configuration NTP peut échouer s'il y a une différence de temps supérieure à 10 minutes entre le serveur NTP et le déploiement vRealize Automation. Pour résoudre ce problème, redémarrez le dispositif vRealize Automation.

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.

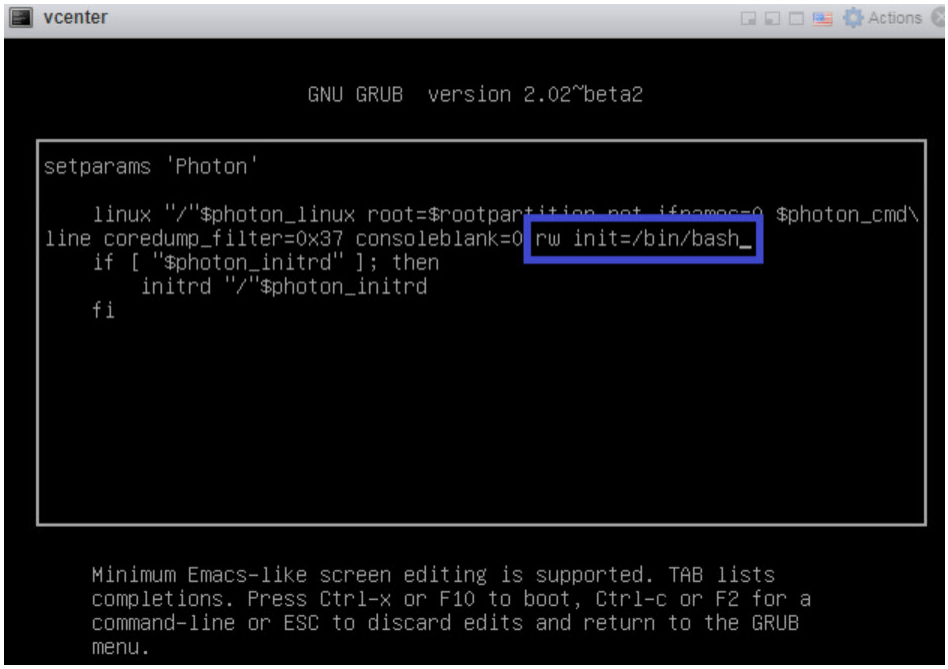
Conditions préalables

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 :



4 Cliquez sur la touche **F10** pour transférer votre modification et redémarrer vRealize Automation.

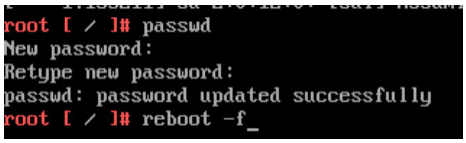
5 Attendez que vRealize Automation redémarre.

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.



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 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 vRealize Suite Lifecycle Manager et de Workspace ONE Access, reportez-vous aux sections suivantes.

- vRealize Suite Lifecycle Manager : reportez-vous à la documentation du produit Lifecycle Manager.
- Workspace ONE Access : reportez-vous aux sections 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.

Avant d'activer 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 Actice Directory associées.

Lorsque de la configuration initiale de l'architecture mutualisée, 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.

Pour plus d'informations sur l'utilisation de vRealize Suite Lifecycle Manager Workspace ONE Access, reportez-vous aux liens de la documentation au début de cette rubrique.

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 Lifecyle 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 3.3.4 ou antérieure.
- Installez et configurez vRealize Suite Lifecycle Manager version 8.5.

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 équilibrages 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 Access et vRealize Automation.

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 Access SAN sur l'instance de Workspace ONE Access ou le cluster.

4 Dans vRealize Suite Lifecycle Manager, exécutez l'assistant Activer le locataire pour activer la mutualisation 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 Lifecyle 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 :
  - vra-1.example.local
  - vra-2.example.local
  - vra-3.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 créerez 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 équilibrages 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 tentant-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-1.example.local vra-2.example.local vra-3.example.local	`Workspace One Certificate` Nom de l'hôte : WorkspaceOne-1.example.local, WorkspaceOne-2.example.local, WorkspaceOne-3.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.example.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, reportez-vous à Gestion des utilisateurs et des groupes.

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 préconfigurée sur la page Intégrations du locataire par défaut. Les sous-locataires ne dispose d'aucune intégration vRealize Orchestrator pré-enregistrée. Ils ont plusieurs options pour ajouter une intégration vRealize Orchestrator.

- Les sous-locataires peuvent ajouter une intégration avec vRealize Orchestrator intégré en accédant à **Infrastructure > Connections > Intégrations**.

  Note Si vRealize Orchestrator intégré est ajouté en tant qu'intégration à plusieurs locataires, tout le contenu vRealize Orchestrator, y compris l'inventaire du plug-in, est partagé entre ces locataires.

- Les sous-locataires peuvent ajouter une instance externe de vRealize Orchestrator qui utilise 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

Divers services génèrent automatiquement des journaux. Vous pouvez générer des bundles de journaux dans vRealize Automation. Vous pouvez également configurer votre environnement pour qu'il envoie les journaux vers vRealize Log Insight.

Vous pouvez obtenir des informations sur l'emploi de l'utilitaire de ligne de commande `vracli` pour générer des bundles de journaux en utilisant l'argument `--help` dans la ligne de commande `vracli` (par exemple, `vracli log-bundle --help`).

Pour plus d'informations sur l'utilisation de vRealize Log Insight, consultez Configuration du transfert de journaux vers vRealize Log Insight dans vRealize Automation.

Commandes de bundles de journaux

Vous pouvez créer un bundle de journaux qui contiendra tous les journaux générés par les services que vous exécutez. Un bundle de journaux contient tous vos journaux de service et est nécessaire pour le dépannage.

Dans un environnement en cluster (mode de haute disponibilité), exécutez la commande `vracli log-bundle` sur un seul nœud. Les journaux sont extraits de tous les nœuds de l'environnement. Cependant, en cas de problème de mise en réseau ou d'autre problème de cluster, les journaux sont extraits d'autant de nœuds que le nombre de nœuds pouvant être atteints. Par exemple, si un nœud est déconnecté dans un cluster de trois nœuds, les journaux sont collectés uniquement à partir des deux nœuds sains. La sortie de la commande `vracli log-bundle` contient des informations sur les problèmes détectés et leurs étapes de résolution.

- Pour créer un bundle de journaux, connectez-vous par SSH à n'importe quel nœud et exécutez la commande `vracli` suivante :

  ```
  vracli log-bundle
  ```

- Pour modifier la valeur du délai d'expiration pour la collecte des journaux de chaque nœud, exécutez la commande `vracli` suivante :

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

  Par exemple, si votre environnement contient des fichiers journaux volumineux, présente une mise en réseau lente ou une utilisation élevée du CPU, vous pouvez définir le délai d'expiration sur une valeur supérieure à la valeur par défaut de 1 000 secondes.

- Pour configurer d'autres options, telles que le délai d'expiration d'Assembly et l'emplacement du tampon, utilisez la commande help `vracli` suivante :

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

Structure de bundle de journaux

Le bundle de journaux est un fichier .tar horodaté. Le nom du bundle correspond au modèle de fichier `log-bundle-<date>T<time>.tar`, par exemple `log-bundle-20200629T131312.tar`. Un bundle de journaux contient généralement des journaux de tous les nœuds de l'environnement. En cas d'erreur, il contient autant de journaux que possible. Il contient au minimum des journaux du nœud local.

Le bundle de journaux a le contenu suivant :

- Fichier d'environnement

  Le fichier d'environnement contient la sortie de diverses commandes de maintenance Kubernetes. Il fournit des informations sur l'utilisation actuelle des ressources par nœud et par espace. Il contient également des informations sur le cluster et la description de toutes les entités Kubernetes disponibles.

- Journaux d'hôte et configuration

  La configuration de chaque hôte (par exemple, son répertoire `/etc`) et les journaux propres à l'hôte (par exemple `journald`) sont collectés dans un répertoire pour chaque nœud de cluster ou hôte. Le nom du répertoire correspond au nom d'hôte du nœud. Le contenu interne du répertoire correspond au système de fichiers de l'hôte. Le nombre de ces répertoires correspond au nombre de nœuds de cluster.

- Journaux de services

  Les journaux des services Kubernetes se trouvent dans la structure de dossiers suivante :

  - `<hostname>/services-logs/<namespace>/<app-name>/file-logs/<container-name>.log`
  - `<hostname>/services-logs/<namespace>/<app-name>/console-logs/<container-name>.log`

  Exemple de nom de fichier : `my-host-01/services-logs/prelude/vco-app/file-logs/vco-server-app.log`.

  - *hostname* est le nom d'hôte du nœud sur lequel le conteneur d'applications s'exécute ou s'exécutait. En général, il existe une instance pour chaque nœud et chaque service. Par exemple, 3 nœuds = 3 instances.
  - *namespace* est l'espace de noms Kubernetes dans lequel l'application se trouve ou a été déployée. Pour les services orientés utilisateur, cette valeur est `prelude`.
  - *app-name* est le nom de l'application Kubernetes qui a produit les journaux, par exemple `provisioning-service-app`.
  - *container-name* est le nom du conteneur qui a produit les journaux. Certaines applications se composent de plusieurs conteneurs. Par exemple, `vco-app` contient les conteneurs `vco-server-app` et `vco-controlcenter-app`.

- (Hérité) Journaux de l'espace

  Avant les modifications apportées à l'architecture de journalisation dans vRealize Automation 8.2, les journaux de services (décrits dans la puce précédente) se trouvaient dans le répertoire de chaque espace dans le bundle de journaux. Bien que vous puissiez continuer à générer des journaux d'espaces dans le bundle à l'aide de la ligne de commande `vracli log-bundle --include-legacy-pod-logs`, cela n'est pas recommandé, car toutes les informations de journalisation résident déjà dans les journaux de chaque service. L'inclusion de journaux d'espace peut inutilement augmenter le temps et l'espace requis pour générer le bundle de journaux.

Réduction de la taille du bundle de journaux

Pour générer un bundle de journaux plus petit, utilisez l'une des commandes `vracli log-bundle` suivantes :

- `vracli log-bundle --since-days n`

  Utilisez cette commande pour collecter uniquement les fichiers journaux générés au cours des derniers jours. Sinon, les journaux sont conservés et collectés pendant 7 jours. Par exemple :

  ```
  vracli log-bundle --since-days 3
  ```

- `vracli log-bundle --services service_A,service_B,service_C`

  Utilisez cette commande pour collecter uniquement les journaux des services fournis nommés. Par exemple :

```
vracli log-bundle --services ebs-app,vco-app
```

- `vracli log-bundle --skip-heap-dumps`

  Utilisez cette commande pour exclure tous les vidages de segment de mémoire du bundle de journaux généré.

Afficher les journaux d'un espace de service ou d'une application

Vous pouvez afficher les journaux d'un espace de service ou d'une application à l'aide de la commande `vracli logs <pod_name>`.

Les options de commande suivantes sont disponibles :

- *--service*

  Affiche un journal fusionné pour tous les nœuds de l'application au lieu d'un espace unique.

  Exemple : `vracli logs --service abx-service-app`

- *--tail n*

  Affiche les *n* dernières lignes du journal. La valeur *n* par défaut est 10.

  Exemple : `vracli logs --tail 20 abx-service-app-8598fcd4b4-tjwhk`

- *--file*

  Affiche uniquement le fichier spécifié. Aucun nom de fichier n'est fourni. Tous les fichiers sont affichés.

  Exemple : `vracli logs --file abx-service-app.log abx-service-app-8598fcd4b4-tjwhk`

Comprendre la rotation des journaux

Les journaux de service existent initialement dans un état non compressé. Une fois qu'un agent vRealize Log Insight a traité les données des journal, un travail vRealize Automation `cron` compresse les journaux de service.

Lorsque 70 % de la partition de disque `/var/log` est utilisée, une tâche `cron` de vRealize Automation supprime les journaux de service les plus anciens.

Pour examiner les informations de rotation des journaux, exécutez les commandes `vracli` suivantes.

```
vracli cluster exec -- bash -c 'current_node; vracli disk-mgr; exit 0'
vracli cluster exec -- bash -c 'current_node; service prune-logs status; exit 0'
```

Configuration du transfert de journaux vers vRealize Log Insight dans vRealize Automation

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 vRealize Log Insight REST API. 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 vRealize Log Insight REST API, consultez la documentation de vRealize Log Insight.

Configurez l'agent de journalisation pour qu'il transfère 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`

Note Vous ne pouvez configurer qu'une seule intégration de journalisation à distance. vRealize Log Insight a priorité si un serveur vRealize Log Insight et un serveur Syslog sont disponibles.

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.

Example - check integration configuration

```
$ vracli vrli
No vRLI integration configured

$ vracli vrli
{
    "agentId": "0",
    "environment": "prod",
    "host": "my-vrli.local",
    "port": 9543,
    "scheme": "https",
    "sslVerify": false
}
```

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

Command

```
vracli vrli set [options] IP_OR_URL
```

Note Après l'exécution de la commande, l'agent de journalisation peut prendre jusqu'à 2 minutes pour appliquer la configuration spécifiée.

Arguments

- IP_OR_URL

  Spécifie l'adresse IP ou l'URL du serveur vRealize Log Insight à utiliser pour la publication des journaux. Le port 9543 et https sont utilisés par défaut. Si l'un de ces paramètres doit être modifié, vous pouvez utiliser une URL à la place.

  Note Vous pouvez définir un autre schéma (https est utilisé par défaut) et un autre port (la valeur par défaut pour https est 9543, 9000 pour http) d'hôte à utiliser pour l'envoi des journaux, comme indiqué dans les exemples suivants :

  ```
  vracli vrli set https://IP:9543
  vracli vrli set --insecure IP
  vracli vrli set http://http://IP:9000
  ```

  Le port 9543 pour https et le port 9000 pour http sont utilisés par la REST API d'ingestion de vRealize Log Insight tel que décrit dans les sections *Administration de vRealize Log Insight* et *Ports et interfaces externes* dans la documentation de vRealize Log Insight.

- Options
  - --agent-id SOME_ID

    Définit l'ID de l'agent de journalisation pour ce dispositif. La valeur par défaut est `0`. Utilisé pour identifier l'agent lors de la publication de journaux pour vRealize Log Insight à l'aide de vRealize Log Insight REST API.

- --environment ENV

  Définit un identifiant pour l'environnement actuel. Il sera disponible dans les journaux vRealize Log Insight en tant que balise pour chaque entrée de journal. La valeur par défaut est `prod`.

- --ca-file /path/to/server-ca.crt

  Spécifie un fichier qui contient le certificat de l'autorité de certification (CA) qui a été utilisé pour signer le certificat du serveur vRealize Log Insight. Cela force l'agent de journalisation à approuver l'autorité de certification spécifiée et à l'activer pour vérifier le certificat du serveur vRealize Log Insight s'il a été signé par une autorité non approuvée. Le fichier peut contenir une chaîne de certificats complète pour vérifier le certificat. Dans le cas d'un certificat auto-signé, transmettez le certificat lui-même.

- --ca-cert CA_CERT

  La définition est identique à celle de --ca-file ci-dessus, mais transmet plutôt le certificat (chaîne) en ligne en tant que chaîne.

- --insecure

  Désactive la vérification SSL du certificat de serveur. Cela force l'agent de journalisation à accepter n'importe quel certificat SSL lors de la publication de journaux.

- Options avancées

  - --request-max-size BYTES

    Plusieurs événements de journalisation sont ingérés avec un seul appel d'API. Cet argument contrôle la taille maximale de la charge utile, en octets, pour chaque demande. Les valeurs valides sont comprises entre 4000 et 4000000. La valeur par défaut est 256000. Pour obtenir des informations connexes sur les valeurs autorisées, consultez Ingestion d'événements vRealize Log Insight dans la documentation de vRealize Log Insight REST API. Si cette valeur est trop basse, les événements de journalisation dépassant la taille autorisée risquent d'être perdus.

  - --request-timeout SECONDS

    Un appel à l'API peut se bloquer pour plusieurs raisons, notamment des problèmes de mise en réseau distante, etc. Ce paramètre contrôle le nombre de secondes d'attente d'exécution de chaque opération, par exemple l'ouverture d'une connexion, l'écriture de données ou l'attente d'une réponse, au terme duquel l'appel est reconnu comme ayant échoué. La valeur ne peut pas être inférieure à 1 seconde. La valeur par défaut est 30.

  - --request-immediate-retries RETRIES

    Les journaux sont mis en mémoire tampon dans des blocs agrégés avant d'être envoyés à vRealize Log Insight (voir --buffer-flush-thread-count ci-dessous). Si une demande d'API échoue, le journal est réessayé immédiatement. Le nombre de tentatives immédiates par défaut est 3. Si aucune des nouvelles tentatives n'aboutit, l'intégralité du bloc de journal est restaurée et est retentée ultérieurement.

- --request-http-compress

  Pour réduire les volumes de trafic réseau, vous pouvez appliquer une compression gzip aux demandes envoyées au serveur vRealize Log Insight. Si ce paramètre n'est pas spécifié, aucune compression n'est utilisée.

- --buffer-flush-thread-count THREADS

  Pour de meilleures performances et pour limiter le trafic de mise en réseau, les journaux sont mis en mémoire tampon localement par blocs avant d'être vidés et envoyés au serveur de journalisation. Chaque bloc contient des journaux provenant d'un seul service. Selon votre environnement, les blocs peuvent devenir volumineux et longs à vider. Cet argument contrôle le nombre de blocs pouvant être vidés simultanément. La valeur par défaut est 2.

Note Lors de la configuration de l'intégration sur https, si le serveur vRealize Log Insight est configuré pour utiliser un certificat non approuvé, tel qu'un certificat auto-signé ou un certificat signé par une autorité non approuvée, vous devez utiliser l'une des options `--ca-file`, `--ca-cert` ou `--insecure`. Dans le cas contraire, l'agent de journalisation ne parvient pas à valider l'identité du serveur et n'envoie pas de journaux. Lorsque vous utilisez `--ca-file` ou `--ca-cert`, le certificat du serveur vRealize Log Insight doit être valide pour le nom d'hôte du serveur. Dans tous les cas, vérifiez l'intégration en prévoyant quelques minutes pour le traitement, puis en vérifiant que vRealize Log Insight a bien reçu les 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.

`Examples - Configure or update integration configuration`

Les exemples d'instructions suivants sont présentés dans des lignes de commande distinctes, mais les arguments peuvent être combinés dans une ligne de commande unique. Par exemple, vous pouvez inclure plusieurs arguments lors de l'utilisation de `vracli vrli set {somehost}` ou `vracli vrli set --ca-file path/to/server-ca.crt` pour modifier l'ID d'agent ou les valeurs d'environnement par défaut. Pour plus d'informations, reportez-vous à l'aide en ligne de la commande en exécutant `vracli vrli --help`.

```
$ 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 --request-http-compress
$ vracli vrli set --environment staging my-vrli.local
$ vracli vrli set --environment staging --request-max-size 10000 --request-timeout 120 --
request-immediate-retries 5 --buffer-flush-thread-count 4 my-vrli.local
```

Effacer l'intégration de vRealize Log Insight

`Command`

```
vracli vrli unset
```

Note Après l'exécution de la commande, l'agent de journalisation peut prendre jusqu'à 2 minutes pour appliquer la configuration spécifiée.

`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 disponibles :

- 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.

`Examples - 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.

Note Vous ne pouvez configurer qu'une seule intégration de journalisation à distance. vRealize Log Insight a priorité si un serveur vRealize Log Insight et un serveur Syslog sont disponibles.

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 dans vRealize Automation.

Conditions préalables

Configurez un serveur Syslog distant.

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`.

Utilisation de packs de contenu

Les packs de contenu sont hébergés dans Log Insight et contiennent des tableaux de bord, des champs extraits, des requêtes enregistrées et des alertes associées à un produit ou un ensemble spécifique de journaux. Vous pouvez installer les packs de contenu pris en charge par la communauté depuis VMware Sample Exchange et d'autres packs de contenu depuis le Marketplace du pack de contenu.

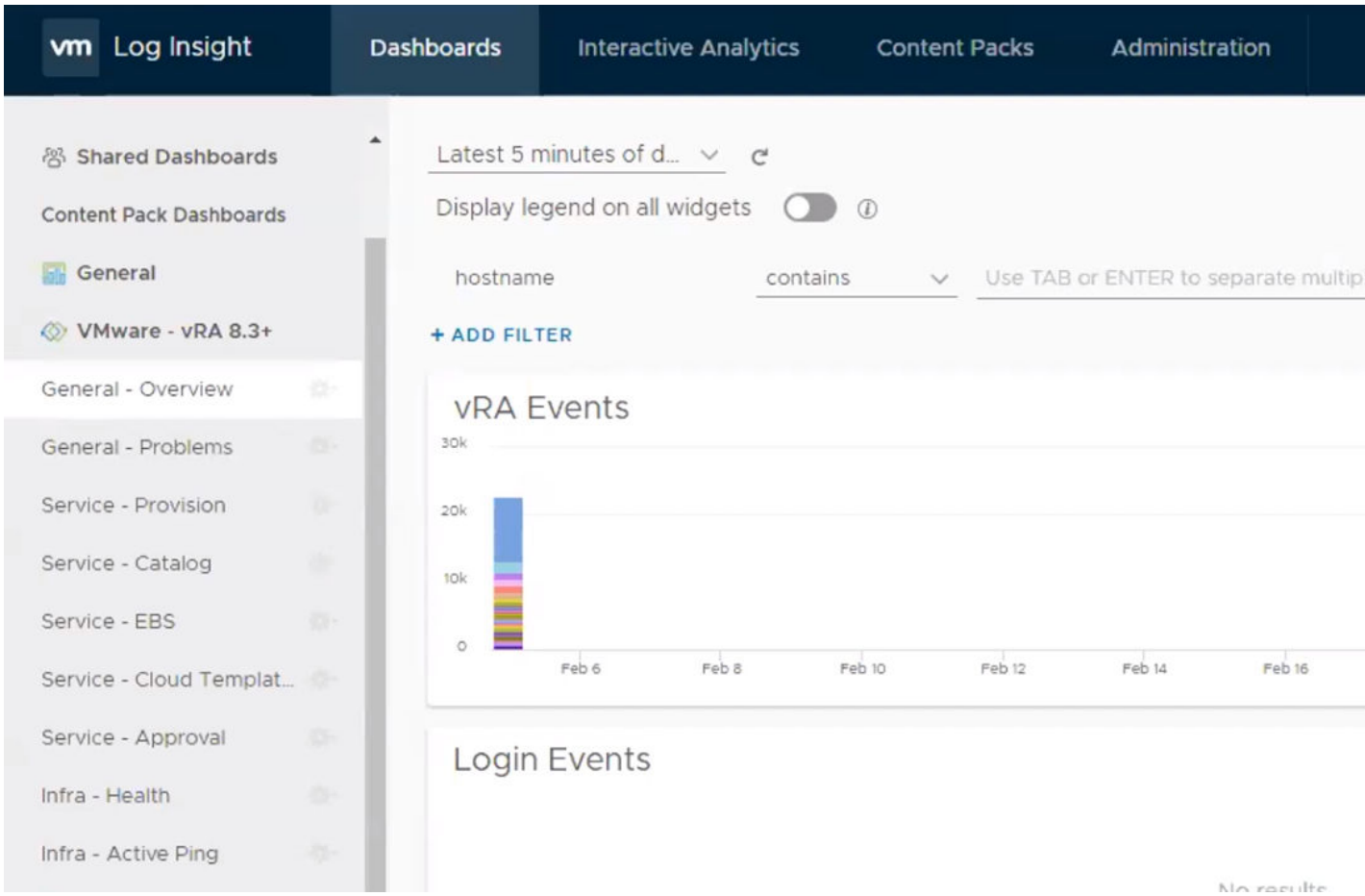
VMware vRealize Log Insight assure la gestion automatisée des journaux via l'agrégation, l'analyse et la recherche, ce qui permet une intelligence opérationnelle et une visibilité à l'échelle de l'entreprise dans des environnements de cloud hybrides dynamiques. Les packs de contenu sont des plug-ins de VMware vRealize Log Insight qui fournissent des connaissances prédéfinies sur des types spécifiques d'événements, tels que des messages de journaux.

Pour télécharger un pack de contenu, dans Log Insight, accédez à **Packs de contenu > Marketplace**. Vous pouvez également importer des packs de contenu en cliquant sur **+ Importer un pack de contenu**.

Pack de contenu vRA 8.x

Le pack de contenu VMware vRealize Automation fournit un résumé consolidé des événements de journaux dans tous les composants de l'environnement vRA. Il inclut plusieurs tableaux de bord qui fournissent une présentation générale, des informations sur les erreurs et les opérations, ainsi que la santé globale de votre instance de vRA. Ces tableaux de bord sont répertoriés dans l'onglet **Tableau de bord** avec tous les autres tableaux de bord Log Insight. Une fois chargés, les tableaux de bord nécessitent jusqu'à 30 secondes pour renseigner les mesures.

Note Vous ne pouvez pas mettre à niveau un pack de contenu vRA 7.5+ vers un pack de contenu vRA 8.3. Vous devez installer le pack de contenu vRA 8.3. Une fois installés, les packs de contenu 8.3 et 7.5 fonctionnent séparément.



Le pack de contenu vRealize Automation inclut les tableaux de bord ci-dessous :

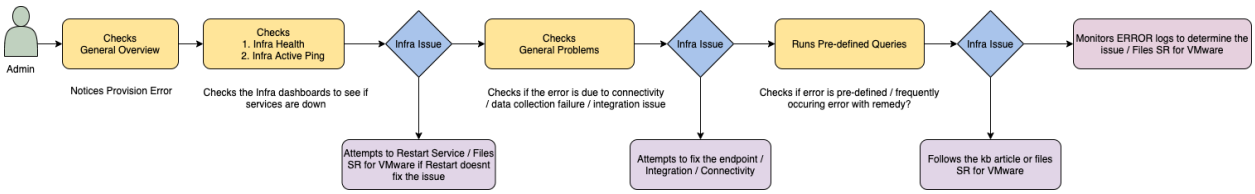
- Général - Présentation : capture un aperçu des mesures de haut niveau pour vRA.
- Général - Problèmes :
- Service - Provision : capture les problèmes liés au service de provisionnement.
- Service - Catalogue : capture les problèmes liés au service de catalogue.
- Service - EBS : capture les problèmes liés au service Event Broker.

- Service - Modèles de cloud : capture les erreurs et les mesures liées aux modèles de cloud Cloud Assembly, aux ressources personnalisées et aux actions sur les ressources.
- Service - Approbation : capture les erreurs et les mesures liées aux approbations.
- Infrastructure - Santé : capture des informations lors des redémarrages des espaces dans le temps. Ce tableau de bord est essentiel pour détecter les pannes de ressources.
- Infrastructure - Ping actif : capture l'URL de contrôle de santé dans le temps.

Chaque tableau de bord contient des widgets individuels qui fournissent des analyses plus axées.

Pour afficher le type d'analyse effectué dans chaque widget, cliquez sur l'icône d'information .

En tant qu vRealize Automation, vous pouvez suivre ce workflow de pack de contenu général pour identifier les erreurs et résoudre les problèmes.



Pour plus d'informations sur le pack de contenu vRealize Automation 8.3, reportez-vous aux sections Pack de contenu de vRealize Automation 8.3+ Log Insight et Configuration du transfert de journaux vers vRealize Log Insight.

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
`frequency.dow=<day-of-week>`	Jour de la collecte de données.
`frequency.hod=<hour-of-day>`	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.