

Administration de vRealize Automation

21 décembre 2020

vRealize Automation 8.0

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

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

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

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

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

Table des matières

1	Administration de vRealize Automation	4
2	Administration des utilisateurs	5
	Activation de groupes Active Directory dans vRealize Automation pour les projets	6
	Suppression d'utilisateurs dans vRealize Automation	7
	Modification des rôles d'utilisateur dans vRealize Automation	7
	Modification des attributions de rôles de groupe dans vRealize Automation	8
3	Maintenance de votre dispositif	10
	Démarrage et arrêt de vRealize Automation	10
	Activation de la synchronisation de l'heure	12
	Désactivation de la synchronisation de l'heure	13
	Réinitialisation du mot de passe racine	14
4	Utilisation des journaux	16
	Utilisation des journaux et des bundles de journaux	16
	Configuration du transfert de journaux vers vRealize Log Insight	18
5	Participation au Programme d'amélioration du produit	23
	Rejoindre ou quitter le programme	23
	Configuration de l'heure de collecte des données pour le programme	24

Administration de vRealize Automation

1

Bien que la plupart des tâches d'administration de vRealize Automation s'effectuent à l'aide de VMware vRealize Suite Lifecycle Manager, ce guide décrit des tâches importantes de gestion des utilisateurs et du système que vous pouvez effectuer dans vRealize Automation.

Pour plus d'informations sur l'utilisation de vRealize Suite Lifecycle Manager, reportez-vous à [Installation, mise à niveau et gestion de vRealize Suite Lifecycle Manager](#).

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 n'est pas prise en charge par vRealize Automation 8.0.0. Pour utiliser vRealize Automation dans des scénarios de récupération d'urgence, procédez à la mise à niveau vers vRealize Automation 8.0.1 ou version ultérieure.

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 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.

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

Il existe trois types de rôles dans vRealize Automation : les rôles d'organisation, les rôles de service et les rôles de projet. Pour vRealize Automation Cloud Assembly, Service Broker et Code Stream, les rôles de niveau utilisateur peuvent généralement utiliser des ressources, alors que les rôles de niveau administrateur sont requis pour créer et configurer des ressources. Les rôles d'organisation définissent les autorisations dans le locataire ; les propriétaires de l'organisation possèdent des autorisations de niveau administrateur, alors que les membres de l'organisation disposent d'autorisations au niveau utilisateur. Les propriétaires de l'organisation peuvent ajouter et gérer d'autres utilisateurs.

Rôles d'organisation	Rôles de service
■ Propriétaire de l'organisation	■ Administrateur de Cloud Assembly
■ Membre de l'organisation	■ Utilisateur de Cloud Assembly
	■ Administrateur de Service Broker
	■ Utilisateur 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 sur l'utilisation de LCM et de Workspace ONE Access, reportez-vous à [Gestion des utilisateurs avec VMware Identity Manager](#).

Ce chapitre contient les rubriques suivantes :

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

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 Tapez 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.

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](#)
- [Activation de la synchronisation de l'heure avec vRealize Automation](#)
- [Désactivation de la synchronisation de l'heure](#)
- [Réinitialisation du mot de passe racine pour vRealize Automation](#)

Démarrage et arrêt de vRealize Automation

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

Arrêter vRealize Automation

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

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

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

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

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

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

- 3 Arrêtez les dispositifs vRealize Automation.

Votre déploiement de vRealize Automation est maintenant arrêté.

Démarrer vRealize Automation

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

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

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

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

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

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

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

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

Redémarrer vRealize Automation

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

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

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

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

Activation de la synchronisation de l'heure avec vRealize Automation

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

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

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

Procédure

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

2 Activez NTP avec ESXi.

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

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

3 Activez NTP avec systemd.

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

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

- b Exécutez la commande `vracli ntp apply`.

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

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

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

Désactivation de la synchronisation de l'heure

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

Conditions préalables

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

Procédure

- 1 Connectez-vous à la ligne de commande du dispositif vRealize Automation en tant qu'utilisateur **racine**.
- 2 Désactivez une configuration NTP ESXi.
 - a Exécutez la commande `vracli ntp esxi --disable`.
 - b Exécutez la commande `vracli ntp apply`.

La configuration NTP ESXi est désactivée.

- 3 Désactivez une configuration NTP systemd.
 - a Exécutez la commande `vracli ntp systemd --disable FQDN_or_IP_of_systemd_server`.
 - b Exécutez la commande `vracli ntp apply`.

La configuration NTP systemd est désactivée.

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

Réinitialisation du mot de passe racine pour vRealize Automation

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

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

Conditions préalables

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

Procédure

- 1 Arrêter et démarrez vRealize Automation en suivant la procédure décrite dans [Démarrage et arrêt de vRealize Automation](#).
- 2 Lorsque la fenêtre de ligne de commande du système d'exploitation Photon s'affiche, entrez `e` et appuyez sur la touche **Entrée** pour ouvrir l'éditeur du menu de démarrage GNU GRUB.

- 3 Dans l'éditeur GNU GRUB, entrez `rw init=/bin/bash` à la fin de la ligne commençant par `linux` `"/" $photon_linux root=rootpartition` comme indiqué ci-dessous :

```

GNU GRUB  version 2.02~beta2

setparams 'Photon'

  linux "/"$photon_linux root=$rootpartition not ifnames=0 $photon_cmd\
line coredump_filter=0x37 consoleblank=0 rw init=/bin/bash_
  if [ "$photon_initrd" ]; then
    initrd "$photon_initrd"
  fi

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

```

- 4 Cliquez sur la touche **F10** pour transférer votre modification et redémarrer vRealize Automation.
- 5 Attendez que vRealize Automation redémarre.
- 6 À l'invite `root [/]#`, entrez `passwd` et appuyez sur la touche **Entrée**.
- 7 À l'invite `New password:`, entrez votre nouveau mot de passe et appuyez sur la touche **Entrée**.
- 8 À l'invite `Retype new password:`, entrez une nouvelle fois votre nouveau mot de passe et appuyez sur la touche **Entrée**.
- 9 À l'invite `root [/]#`, entrez `reboot -f` et appuyez sur la touche **Entrée** pour terminer le processus de réinitialisation du mot de passe racine.

```

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

```

Étape suivante

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

Utilisation des journaux dans vRealize Automation

4

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

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

Ce chapitre contient les rubriques suivantes :

- [Utilisation des journaux et des bundles de journaux dans vRealize Automation](#)
- [Configuration du transfert de journaux vers vRealize Log Insight](#)

Utilisation des journaux et des bundles de journaux dans vRealize Automation

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

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

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

Commandes de bundles de journaux

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

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

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

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

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

- Créez un bundle de journaux simple.

```
vracli log-bundle
```

- Créer un bundle de journaux de stockage à froid :

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

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

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

Structures de bundles de journaux

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

- Bundles de journaux normaux

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

- Journaux d'hôte et configuration

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

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

- Journaux d'espace

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

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

- Fichier d'environnement

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

- Bundles de journaux de secours

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

- Journaux de conteneur de secours

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

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

- Stockage à froid de secours

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

Configuration du transfert de journaux vers vRealize Log Insight

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

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

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

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

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

Vérifier la configuration existante de vRealize Log Insight

Command

```
vracli vrli
```

Arguments

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

Output

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

Exit codes

Les codes de sortie suivants sont possibles :

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

Example – check integration configuration

```
$ vracli vrli
No vRLI integration configured

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

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

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

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

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

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

Command

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

Arguments

Les arguments de ligne de commande suivants sont disponibles :

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

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

Output

Aucune sortie n'est attendue.

Exit codes

Les codes de sortie suivants sont possibles :

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

Exemples – Configure or update integration configuration

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

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

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

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

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

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

Effacer l'intégration de vRealize Log Insight

Command

```
vracli vrli unset
```

Arguments

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

Output

La sortie de la confirmation est au format texte simple.

Exit codes

Les codes de sortie suivants sont possibles :

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

Examples – Clear integration

```
$ vracli vrli unset  
Clearing vRLI integration configuration
```

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

Participation au Programme d'amélioration du produit pour vRealize Automation

5

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 `vraccli ceip off`.
- 3 Pour redémarrer les services vRealize Automation, exécutez la commande `/opt/scripts/deploy.sh`.

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

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

Procédure

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

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

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

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

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