

Administering vRealize Log Insight

12-OCT-2017

vRealize Log Insight 4.5



vmware®

You can find the most up-to-date technical documentation on the VMware website at:

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

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

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

Copyright © 2014–2017 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

Administration de vRealize Log Insight 7

Updated Information for *Administration de vRealize Log Insight* 8

1 Mise à niveau de vRealize Log Insight 9

Chemin de mise à niveau de vRealize Log Insight 9

Mise à niveau vers vRealize Log Insight 4.5 10

Mise à niveau vers vRealize Log Insight 4.3 11

Mise à niveau vers vRealize Log Insight 4.0 12

Mise à niveau vers vRealize Log Insight 3.6 13

2 Gestion des comptes d'utilisateur vRealize Log Insight 15

Présentation de la gestion des utilisateurs 16

Contrôle d'accès basé sur les rôles 16

Créer un compte d'utilisateur dans vRealize Log Insight 17

Configurer l'accès de VMware Identity Manager à des groupes Active Directory pour
vRealize Log Insight 18

Importer un groupe Active Directory dans vRealize Log Insight 20

Authentification d'utilisateurs avec l'appartenance au groupe inter-domaines 21

Définir un jeu de données 22

Créer et modifier des rôles 23

Supprimer un compte d'utilisateur à partir de vRealize Log Insight 24

3 Configuration de l'authentification 25

Activer l'authentification des utilisateurs via VMware Identity Manager 25

Permettre l'authentification utilisateur à travers Active Directory 27

Configurer le protocole à utiliser pour Active Directory 28

4 Configuration de vRealize Log Insight 30

Limites de configuration de vRealize Log Insight 31

Configuration des paramètres du dispositif virtuel 32

Configurer le mot de passe SSH racine du dispositif virtuel vRealize Log Insight 32

Modifier les paramètres réseau du vApp vRealize Log Insight 33

Augmenter la capacité de stockage du dispositif virtuel vRealize Log Insight 34

Ajouter de la mémoire et des CPU au dispositif virtuel vRealize Log Insight 36

Attribuer une licence permanente à vRealize Log Insight 36

Stratégie de stockage des journaux 37

Gestion des notifications système	37
Notifications système dans vRealize Log Insight	38
Configuration de notifications système vRealize Log Insight	47
Ajouter une destination de transfert d'événements de vRealize Log Insight	50
Configurer le transfert d'événements de vRealize Log Insight avec SSL	53
Synchroniser l'heure sur le dispositif virtuel vRealize Log Insight	53
Configurer le serveur SMTP pour vRealize Log Insight	54
Installer un certificat SSL personnalisé	55
Générer un certificat autosigné	57
Générer une demande de signature de certificat	58
Demander la signature d'une autorité de certification	59
Concaténer les fichiers de certificat	59
Télécharger un certificat signé	60
Configurer la connexion SSL entre le serveur vRealize Log Insight et Log Insight Agents	60
Modifier le délai d'expiration par défaut des sessions Web de vRealize Log Insight	64
Archives	65
Activer ou désactiver l'archivage des données dans vRealize Log Insight	65
Format des fichiers d'archives de vRealize Log Insight	66
Importer une archive vRealize Log Insight dans vRealize Log Insight	67
Exporter une archive Log Insight vers un fichier texte brut ou au format JSON	68
Redémarrer le service vRealize Log Insight	69
Mettre le dispositif virtuel vRealize Log Insight hors tension	70
Télécharger un bundle de support vRealize Log Insight	70
Rejoindre ou quitter le programme d'amélioration du produit VMware	71
5 Configuration des clusters vRealize Log Insight	73
Ajouter un nœud travailleur à un cluster vRealize Log Insight	73
Déployer le dispositif virtuel vRealize Log Insight	74
Rejoindre un déploiement existant	77
Supprimer un nœud travailleur d'un cluster vRealize Log Insight	78
Utilisation de l'équilibrage de charge intégrée	79
Activer l'équilibrage de charge intégrée	80
Interroger les résultats des vérifications du cluster en production	81
6 Ports et interfaces externes	82
7 Surveiller l'état des agents Windows et Linux de vRealize Log Insight	86
8 Activer la mise à jour automatique des agents à partir du serveur	87
9 Utilisation des groupes d'agents	88
Fusion de la configuration d'un groupe d'agents	89

	Créer un groupe d'agents	89
	Modifier un groupe d'agents	90
	Ajouter un groupe d'agents de pack de contenu en tant que groupe d'agents	90
	Supprimer un groupe d'agents	91
10	Configuration et utilisation de vRealize Log Insight Importer	92
	À propos du fichier de manifeste de vRealize Log Insight Importer	93
	Installer, configurer et exécuter vRealize Log Insight Importer	94
	Exemples de configuration de fichier de manifeste vRealize Log Insight Importer	96
	Paramètres de configuration de vRealize Log Insight Importer	97
11	Surveillance de vRealize Log Insight	99
	Vérifier la santé du dispositif virtuel vRealize Log Insight	99
	Surveiller les hôtes qui envoient des événements de journaux	100
12	Intégration de vRealize Log Insight à des produits VMware	101
	Connecter vRealize Log Insight à un environnement vSphere	102
	vRealize Log Insight en tant que serveur Syslog	104
	Configurer un hôte ESXi pour le transfert des événements de journaux à vRealize Log Insight	104
	Modifier une configuration d'hôte ESXi pour le transfert des événements de journaux à vRealize Log Insight	106
	Événements de notification vRealize Log Insight dans vRealize Operations Manager	107
	Configurer vRealize Log Insight pour l'extraction des événements, des tâches et des alarmes d'une instance de vCenter Server	108
	Utilisation de vRealize Operations Manager avec vRealize Log Insight	109
	Conditions requises pour l'intégration à vRealize Operations Manager	109
	Configurer vRealize Log Insight pour envoyer des événements de notification à vRealize Operations Manager	111
	Activer le lancement contextuel de vRealize Log Insight dans vRealize Operations Manager	112
	Désactiver le lancement contextuel de vRealize Log Insight dans vRealize Operations Manager	117
	Ajouter un chemin et un domaine de recherche DNS	118
	Supprimer l'adaptateur vRealize Log Insight	118
	Pack de contenu de vRealize Operations Manager pour vRealize Log Insight	120
13	Considérations en matière de sécurité de vRealize Log Insight	121
	Ports et interfaces externes	121
	Fichiers de configuration de vRealize Log Insight	125
	Clé publique, certificat et keystore de vRealize Log Insight	125
	Fichier de licence et CLUF de vRealize Log Insight	126
	Fichiers journaux de vRealize Log Insight	126
	Comptes d'utilisateurs vRealize Log Insight	128

Recommandations relatives au pare-feu pour vRealize Log Insight	129
Correctifs et mises à jour de sécurité	130

14 Sauvegarde, restauration et récupération d'urgence 131

Présentation des opérations de sauvegarde, restauration et récupération d'urgence	131
Utilisation d'adresses IP statiques et de noms de domaines complets	132
Planification et préparation	133
Sauvegarder des nœuds et des clusters	134
Agents de sauvegarde Linux ou Windows	135
Restaurer des nœuds et des clusters	136
Modification de configurations après restauration	137
Restaurer sur le même hôte	137
Restaurer sur un hôte différent	138
Vérifier les restaurations	141
Récupération d'urgence	142

15 Dépannage de vRealize Log Insight 143

L'espace disque de vRealize Log Insight est épuisé	143
L'importation de données archivées peut échouer	144
Créer un bundle de support de vRealize Log Insight à l'aide de la console du dispositif virtuel	144
Réinitialiser le mot de passe de l'utilisateur Admin	145
Réinitialiser le mot de passe de l'utilisateur racine	146
Des alertes n'ont pas pu être envoyées à vRealize Operations Manager	147
Impossible de se connecter à l'aide des informations d'identification Active Directory	148
SMTP ne fonctionne pas lorsque l'option STARTTLS est activée	149
La mise à niveau échoue du fait que la signature du fichier .pak ne peut pas être validée	149
La mise à niveau échoue en générant une erreur de serveur interne	150

Administration de vRealize Log Insight

Le document *Administration de vRealize Log Insight* fournit des informations sur l'administration de VMware® vRealize™ Log Insight™, la gestion des comptes d'utilisateurs et l'intégration de Log Insight Agents à d'autres produits VMware. Il inclut également des informations sur la gestion de la sécurité des produits et sur la mise à niveau de votre déploiement.

Elles sont destinées aux administrateurs Windows ou Linux expérimentés qui maîtrisent les technologies de machine virtuelle et les opérations de centre de données.

Updated Information for *Administration de vRealize Log Insight*

Administration de vRealize Log Insight is updated with each release of the product or when necessary.

This table provides the update history of *Administration de vRealize Log Insight*.

Revision	Description
10-OCT-2017	<ul style="list-style-type: none">■ Removal of note about deprecation of support for Active Directory.■ Minor bug fixes.
05-SEP-2017	<ul style="list-style-type: none">■ Clarification of hardware requirements.
002541-1	<ul style="list-style-type: none">■ Revisions provide clarification of support status for external load balancers and native Active Directory use. See Utilisation de l'équilibrage de charge intégrée and Chapter 3 Configuration de l'authentification.
002541-0	Initial release.

Mise à niveau de vRealize Log Insight

1

En fonction de la version actuelle de vRealize Log Insight, vous pouvez mettre à niveau vers une version plus récente.

Ce chapitre aborde les rubriques suivantes :

- [Chemin de mise à niveau de vRealize Log Insight](#)
- [Mise à niveau vers vRealize Log Insight 4.5](#)
- [Mise à niveau vers vRealize Log Insight 4.3](#)
- [Mise à niveau vers vRealize Log Insight 4.0](#)
- [Mise à niveau vers vRealize Log Insight 3.6](#)

Chemin de mise à niveau de vRealize Log Insight

Le chemin et la procédure de mise à niveau à suivre varient en fonction de la version installée de vRealize Log Insight que vous souhaitez mettre à niveau.

Vous pouvez également vérifier les chemins de mise à niveau pris en charge à l'aide de la fonctionnalité **Chemin de mise à niveau** disponible sur le site des [Matrices d'interopérabilité des produits VMware](#).

Les mises à niveau de vRealize Log Insight sont incrémentielles. Vous devez effectuer la mise à niveau à chaque version intermédiaire.

Tableau 1-1. Chemins de mise à niveau pris en charge

Mettre à niveau depuis	Mettre à niveau vers	Procédure
vRealize Log Insight 4.3	vRealize Log Insight 4.5	Reportez-vous à Mise à niveau vers vRealize Log Insight 4.5
vRealize Log Insight 4.0	vRealize Log Insight 4.3	Reportez-vous à Mise à niveau vers vRealize Log Insight 4.3
vRealize Log Insight 3.6	vRealize Log Insight 4.0	Reportez-vous à Mise à niveau vers vRealize Log Insight 4.0 .
vRealize Log Insight 3.3	vRealize Log Insight 3.6	Reportez-vous à Mise à niveau vers vRealize Log Insight 3.6 .

Mise à niveau vers vRealize Log Insight 4.5

Vous pouvez automatiquement mettre à niveau un cluster vers vRealize Log Insight 4.5.

La mise à niveau de vRealize Log Insight doit se faire à partir du nom de domaine complet du nœud maître. La mise à niveau à l'aide de l'adresse IP de l'équilibrage de charge intégré n'est pas prise en charge.


Au cours de la mise à niveau, le nœud maître est mis à niveau et redémarre. Ensuite, les nœuds de cluster sont mis à niveau successivement. Vous pouvez voir l'état actuel de la mise à niveau propagée sur la page **Administration > Cluster**. Si l'équilibrage de charge intégré est configuré, ses adresses IP sont migrées parmi les nœuds de cluster. Ainsi, les services de cluster, y compris l'interface utilisateur, l'API et l'ingestion d'événements entrants, restent disponibles tout au long de la mise à niveau propagée. Des détails sont inscrits dans le fichier `upgrade.log` sur chaque nœud individuel. Une notification système est envoyée lorsque la mise à niveau est bien terminée.

Si un problème touchant un ou plusieurs nœuds lors du processus de mise à niveau survient, tout le cluster est automatiquement restauré à la version opérationnelle d'origine. Comme les modifications apportées à la configuration après le début de la mise à niveau peuvent être incohérentes ou non valides, la configuration repasse à un état correct connu, capturé avant la mise à niveau. Aucun événement ingéré n'est perdu. La progression est inscrite dans le fichier `rollback.log` sur chaque nœud individuel. Une notification système est envoyée lorsque la restauration est terminée. Une fois que le problème est examiné et corrigé, vous pouvez retenter la mise à niveau.

Prérequis

- Vérifiez que vous appliquez la mise à niveau pour un chemin de mise à niveau pris en charge. Reportez-vous à [Chemin de mise à niveau de vRealize Log Insight](#).
- Create a snapshot or backup copy of the vRealize Log Insight virtual appliance.
- Obtenez une copie du fichier `.pak` du bundle de mise à niveau de vRealize Log Insight pour voir la version vers laquelle vous effectuez la mise à niveau.
- Verify that you are logged in to the vRealize Log Insight *portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Cluster**.
- 3 Cliquez sur **Mettre niveau à partir de PAK** pour télécharger le fichier `.pak`.
- 4 Accept the new EULA to complete the upgrade procedure.

Suivant

Une fois le processus de mise à niveau du nœud maître effectué, vous pouvez afficher le processus de mise à niveau restant, ce qui est automatique.

Vérifiez le message électronique envoyé à Admin pour confirmer l'aboutissement de la mise à niveau.

Mise à niveau vers vRealize Log Insight 4.3

Vous pouvez automatiquement mettre à niveau un cluster vers vRealize Log Insight 4.3.

La mise à niveau de vRealize Log Insight doit se faire à partir du nom de domaine complet du nœud maître. La mise à niveau à l'aide de l'adresse IP de l'équilibrage de charge intégré n'est pas prise en charge.


Au cours de la mise à niveau, le nœud maître est mis à niveau et redémarre. Ensuite, les nœuds de cluster sont mis à niveau successivement. Vous pouvez voir l'état actuel de la mise à niveau propagée sur la page **Administration > Cluster**. Si l'équilibrage de charge intégré est configuré, ses adresses IP sont migrées parmi les nœuds de cluster. Ainsi, les services de cluster, y compris l'interface utilisateur, l'API et l'ingestion d'événements entrants, restent disponibles tout au long de la mise à niveau propagée. Des détails sont inscrits dans le fichier `upgrade.log` sur chaque nœud individuel. Une notification système est envoyée lorsque la mise à niveau est bien terminée.

Si un problème touchant un ou plusieurs nœuds lors du processus de mise à niveau survient, tout le cluster est automatiquement restauré à la version opérationnelle d'origine. Comme les modifications apportées à la configuration après le début de la mise à niveau peuvent être incohérentes ou non valides, la configuration repasse à un état correct connu, capturé avant la mise à niveau. Aucun événement ingéré n'est perdu. La progression est inscrite dans le fichier `rollback.log` sur chaque nœud individuel. Une notification système est envoyée lorsque la restauration est terminée. Une fois que le problème est examiné et corrigé, vous pouvez retenter la mise à niveau.

Prérequis

- Vérifiez que vous appliquez la mise à niveau pour un chemin de mise à niveau pris en charge. Reportez-vous à [Chemin de mise à niveau de vRealize Log Insight](#).
- Create a snapshot or backup copy of the vRealize Log Insight virtual appliance.
- Obtenez une copie du fichier `.pak` du bundle de mise à niveau de vRealize Log Insight pour voir la version vers laquelle vous effectuez la mise à niveau.
- Verify that you are logged in to the vRealize Log Insight *portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Cluster**.
- 3 Cliquez sur **Mettre niveau à partir de PAK** pour télécharger le fichier `.pak`.

- 4 Accept the new EULA to complete the upgrade procedure.

Suivant

Une fois le processus de mise à niveau du nœud maître effectué, vous pouvez afficher le processus de mise à niveau restant, ce qui est automatique.

Vérifiez le message électronique envoyé à Admin pour confirmer l'aboutissement de la mise à niveau.

Mise à niveau vers vRealize Log Insight 4.0

Vous pouvez automatiquement mettre à niveau un cluster vers vRealize Log Insight 4.0.

La mise à niveau de vRealize Log Insight doit se faire à partir du nom de domaine complet du nœud maître. La mise à niveau à l'aide de l'adresse IP de l'équilibrage de charge intégré n'est pas prise en charge.


Au cours de la mise à niveau, le nœud maître est mis à niveau et redémarre. Ensuite, les nœuds de cluster sont mis à niveau successivement. Vous pouvez voir l'état actuel de la mise à niveau propagée sur la page **Administration > Cluster**. Si l'équilibrage de charge intégré est configuré, ses adresses IP sont migrées parmi les nœuds de cluster. Ainsi, les services de cluster, y compris l'interface utilisateur, l'API et l'ingestion d'événements entrants, restent disponibles tout au long de la mise à niveau propagée. Des détails sont inscrits dans le fichier `upgrade.log` sur chaque nœud individuel. Une notification système est envoyée lorsque la mise à niveau est bien terminée.

Si un problème touchant un ou plusieurs nœuds lors du processus de mise à niveau survient, tout le cluster est automatiquement restauré à la version opérationnelle d'origine. Comme les modifications apportées à la configuration après le début de la mise à niveau peuvent être incohérentes ou non valides, la configuration repasse à un état correct connu, capturé avant la mise à niveau. Aucun événement ingéré n'est perdu. La progression est inscrite dans le fichier `rollback.log` sur chaque nœud individuel. Une notification système est envoyée lorsque la restauration est terminée. Une fois que le problème est examiné et corrigé, vous pouvez retenter la mise à niveau.

Prérequis

- Vérifiez que vous appliquez la mise à niveau pour un chemin de mise à niveau pris en charge. Reportez-vous à [Chemin de mise à niveau de vRealize Log Insight](#).
- Create a snapshot or backup copy of the vRealize Log Insight virtual appliance.
- Obtenez une copie du fichier `.pak` du bundle de mise à niveau de vRealize Log Insight pour voir la version vers laquelle vous effectuez la mise à niveau.
- Verify that you are logged in to the vRealize Log Insight *portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Cluster**.

- 3 Cliquez sur **Mettre niveau à partir de PAK** pour télécharger le fichier .pak.
- 4 Accept the new EULA to complete the upgrade procedure.

Suivant

Une fois le processus de mise à niveau du nœud maître effectué, vous pouvez afficher le processus de mise à niveau restant, ce qui est automatique.

Vérifiez le message électronique envoyé à Admin pour confirmer l'aboutissement de la mise à niveau.

Mise à niveau vers vRealize Log Insight 3.6

Vous pouvez automatiquement mettre à niveau un cluster vers vRealize Log Insight 3.6.

La mise à niveau de vRealize Log Insight doit se faire à partir du nom de domaine complet du nœud maître. La mise à niveau à l'aide de l'adresse IP de l'équilibrage de charge intégré n'est pas prise en charge.

Au cours de la mise à niveau, le nœud maître est mis à niveau et redémarre. Ensuite, les nœuds de cluster sont mis à niveau successivement. Vous pouvez voir l'état actuel de la mise à niveau propagée sur la page **Administration > Cluster**. Si l'équilibrage de charge intégré est configuré, ses adresses IP sont migrées parmi les nœuds de cluster. Ainsi, les services de cluster, y compris l'interface utilisateur, l'API et l'ingestion d'événements entrants, restent disponibles tout au long de la mise à niveau propagée. Des détails sont inscrits dans le fichier `upgrade.log` sur chaque nœud individuel. Une notification système est envoyée lorsque la mise à niveau est bien terminée.

Si un problème touchant un ou plusieurs nœuds lors du processus de mise à niveau survient, tout le cluster est automatiquement restauré à la version opérationnelle d'origine. Comme les modifications apportées à la configuration après le début de la mise à niveau peuvent être incohérentes ou non valides, la configuration repasse à un état correct connu, capturé avant la mise à niveau. Aucun événement ingéré n'est perdu. La progression est inscrite dans le fichier `rollback.log` sur chaque nœud individuel. Une notification système est envoyée lorsque la restauration est terminée. Une fois que le problème est examiné et corrigé, vous pouvez retenter la mise à niveau.

Prérequis

- Vérifiez que vous appliquez la mise à niveau pour un chemin de mise à niveau pris en charge. Reportez-vous à [Chemin de mise à niveau de vRealize Log Insight](#).
- Create a snapshot or backup copy of the vRealize Log Insight virtual appliance.
- Obtenez une copie du fichier .pak du bundle de mise à niveau de vRealize Log Insight pour voir la version vers laquelle vous effectuez la mise à niveau.
- Verify that you are logged in to the vRealize Log Insight *portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.

- 2 Under Management, click **Cluster**.
- 3 Cliquez sur **Mettre niveau à partir de PAK** pour télécharger le fichier .pak.
- 4 Accept the new EULA to complete the upgrade procedure.

Suivant

Une fois le processus de mise à niveau du nœud maître effectué, vous pouvez afficher le processus de mise à niveau restant, ce qui est automatique.

Vérifiez le message électronique envoyé à Admin pour confirmer l'aboutissement de la mise à niveau.

Gestion des comptes d'utilisateur vRealize Log Insight

2

Les utilisateurs Admin peuvent créer des comptes d'utilisateur et des rôles pour offrir un accès à l'interface Web de vRealize Log Insight.

Seuls les utilisateurs disposant de l'autorisation Modifier Admin peuvent créer et modifier les comptes d'utilisateur. Les utilisateurs peuvent cependant modifier leurs propres e-mail et mot de passe de compte sans avoir la permission Modifier Admin.

Ce chapitre aborde les rubriques suivantes :

- [Présentation de la gestion des utilisateurs](#)
- [Contrôle d'accès basé sur les rôles](#)
- [Créer un compte d'utilisateur dans vRealize Log Insight](#)
- [Configurer l'accès de VMware Identity Manager à des groupes Active Directory pour vRealize Log Insight](#)
- [Importer un groupe Active Directory dans vRealize Log Insight](#)
- [Authentification d'utilisateurs avec l'appartenance au groupe inter-domaines](#)
- [Définir un jeu de données](#)
- [Créer et modifier des rôles](#)
- [Supprimer un compte d'utilisateur à partir de vRealize Log Insight](#)

Présentation de la gestion des utilisateurs

Les administrateurs système utilisent une combinaison de noms d'utilisateur, de contrôles d'accès basés sur les rôles, d'autorisations et de jeux de données pour gérer les utilisateurs de vRealize Log Insight. Le contrôle d'accès basé sur les rôles permet aux administrateurs de gérer les utilisateurs et les tâches qu'ils peuvent effectuer.

Les rôles sont des ensembles d'autorisations requises pour effectuer certaines tâches. Les administrateurs système définissent les rôles dans le cadre de la définition des stratégies de sécurité et accordent les rôles aux utilisateurs. Pour modifier les autorisations et les tâches associées à un rôle particulier, l'administrateur système met à jour les paramètres du rôle. Les paramètres mis à jour s'appliquent à l'ensemble des utilisateurs associés à ce rôle.

- Pour autoriser un utilisateur à effectuer une tâche, l'administrateur système lui accorde le rôle correspondant.
- Pour empêcher un utilisateur d'effectuer une tâche, l'administrateur système révoque le rôle correspondant.

La gestion de l'accès, des rôles et des autorisations pour chaque utilisateur est basée sur son compte de connexion utilisateur. Chaque utilisateur peut se voir accorder plusieurs rôles et autorisations.

Les utilisateurs qui ne peuvent ni voir ni accéder à certains objets ou qui ne peuvent pas effectuer certaines opérations n'ont pas reçu l'autorisation de le faire.

Contrôle d'accès basé sur les rôles

Le contrôle d'accès basé sur les rôles permet aux administrateurs système de contrôler l'accès utilisateur à vRealize Log Insight et contrôle les tâches que les utilisateurs peuvent effectuer après leur connexion. Pour mettre en œuvre le contrôle d'accès basé sur les rôles, les administrateurs système associent des autorisations et des rôles à des comptes de connexion d'utilisateur ou révoquent ces autorisations et ces rôles

Utilisateurs

Les administrateurs système peuvent contrôler l'accès et les actions de chaque utilisateur en accordant des autorisations et des rôles au compte de connexion de l'utilisateur et en révoquant ces autorisations et ces rôles.

Autorisations

Les autorisations contrôlent les actions autorisées dans vRealize Log Insight. Les autorisations s'appliquent à des tâches administratives ou utilisateur particulières dans vRealize Log Insight. Par exemple, vous pouvez accorder l'autorisation **Administrateur affichage** pour permettre à un utilisateur de voir les paramètres administratifs de vRealize Log Insight.

Jeux de données

Les jeux de données sont composés d'une série de filtres. Vous pouvez utiliser les jeux de données pour accorder aux utilisateurs un accès à du contenu spécifique en associant un jeu de données à un rôle.

Rôles

Les rôles sont des collections d'autorisations et de jeux de données pouvant être associées à des utilisateurs. Les rôles fournissent un moyen pratique de regrouper toutes les autorisations requises pour effectuer une tâche. Plusieurs rôles peuvent être attribués à un utilisateur.

Créer un compte d'utilisateur dans vRealize Log Insight


Les utilisateurs qui obtiennent le rôle de Super administrateur peuvent créer des comptes d'utilisateurs pour fournir un accès à l'interface utilisateur Web de vRealize Log Insight.

Prérequis

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Vérifiez que vous avez configuré la prise en charge de VMware Identity Manager ou Active Directory si vous créez des comptes d'utilisateur qui recourent à l'un de ces types d'authentification. Voir [Activer l'authentification des utilisateurs via VMware Identity Manager](#) et [Permettre l'authentification utilisateur à travers Active Directory](#)

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Access Control**.
- 3 Cliquez sur **Utilisateurs et groupes**.
- 4 Click **New User**.
- 5 Choisissez une option dans le menu déroulant **Authentification**.
 - Si vous utilisez l'authentification par défaut intégrée, entrez un nom d'utilisateur, un mot de passe et, éventuellement, une adresse e-mail. Copiez le mot de passe dans la zone de texte **Mot de passe** et indiquez-le à l'utilisateur.
 - Si vous utilisez l'authentification Active Directory ou VMware Identity Manager, entrez le domaine auquel appartient l'utilisateur, un nom d'utilisateur et, éventuellement, l'adresse e-mail du compte d'utilisateur.

- 6 From the **Roles** list on the right, select one or more predefined or custom user roles.

Option	Description
User	Users can access the full functionality of vRealize Log Insight. You can view log events, run queries to search and filter logs, import content packs into their own user space, add alert queries, and manage your own user accounts to change a password or email address. Users do not have access to the administration options, cannot share content with other users, cannot modify the accounts of other users, and cannot install a content pack from the Marketplace. However, you can import a content pack into your own user space which is visible only to you.
Dashboard User	Dashboard users can only use the Dashboards page of vRealize Log Insight.
View Only Admin	View Admin users can view Admin information, have full User access, and can edit Shared content.
Super Admin	Super Admin users can access the full functionality of vRealize Log Insight, can administer vRealize Log Insight, and can manage the accounts of all other users.

- 7 Cliquez sur **Enregistrer**.

- Pour l'authentification intégrée, les informations sont enregistrées localement.
- Pour l'authentification VMware Identity Manager, vRealize Log Insight vérifie que VMware Identity Manager est bien synchronisé avec le groupe spécifié et avec son domaine. Si le groupe est introuvable, une boîte de dialogue vous informe que vRealize Log Insight ne peut pas vérifier ce groupe. Vous pouvez enregistrer le groupe sans qu'il n'ait été vérifié ou bien annuler pour corriger le nom du groupe ou le domaine.

Configurer l'accès de VMware Identity Manager à des groupes Active Directory pour vRealize Log Insight

Vous pouvez utiliser des groupes Active Directory avec vRealize Log Insight via l'authentification unique de VMware Identity Manager. Votre site doit être configuré pour l'authentification VMware Identity Manager qui est activée pour la prise en charge d'Active Directory et la synchronisation du serveur doit être en place.

Vous devez également importer des informations sur le groupe dans vRealize Log Insight


Un utilisateur VMware Identity Manager hérite des rôles qui sont attribués à un groupe auquel l'utilisateur appartient, en plus des rôles qui sont attribués à l'utilisateur individuel. Par exemple, un administrateur peut attribuer le rôle **Afficher le compte Admin** au GroupA et attribuer le rôle **Utilisateur** à l'utilisateur Bob. Bob peut également être affecté au GroupA. Lorsque Bob ouvre une session, il hérite du rôle du groupe et dispose des privilèges pour les rôles **Afficher le compte Admin** et **Utilisateur**.

Notez que le groupe n'est pas un groupe VMware Identity Manager local, mais un groupe Active Directory qui est synchronisé avec VMware Identity Manager.

Prérequis

- Vérifiez que vous avez configuré l'attribut UPN (userPrincipalName). Il peut être configuré via l'interface d'administration de VMware Identity Manager dans **Identité et gestion de l'accès > Attributs utilisateur**.
- Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight en tant qu'utilisateur disposant de l'autorisation **Modifier le compte Admin**. Le format de l'URL est `https://log-insight-host` où `log-insight-host` est l'adresse IP ou le nom d'hôte du dispositif virtuel vRealize Log Insight.
- Vérifiez que vous avez configuré la prise en charge de VMware Identity Manager dans vRealize Log Insight. Reportez-vous à [Activer l'authentification des utilisateurs via VMware Identity Manager](#)

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Access Control**.
- 3 Click **Users and Groups**.
- 4 Accédez au tableau des groupes Active Directory, puis cliquez sur **Nouveau groupe**.
- 5 Sélectionnez **VMware Identity Manager** dans le menu déroulant **Type**.
Le nom de domaine par défaut que vous indiquez lors de la configuration de la prise en charge de VMware Identity Manager s'affiche dans la zone de texte **Domaine**.
- 6 Remplacez le nom de domaine par le nom Active Directory du groupe.
- 7 Tapez le nom du groupe que vous voulez ajouter.
- 8 From the **Roles** list on the right, select one or more predefined or custom user roles.

Option	Description
User	Users can access the full functionality of vRealize Log Insight. You can view log events, run queries to search and filter logs, import content packs into their own user space, add alert queries, and manage your own user accounts to change a password or email address. Users do not have access to the administration options, cannot share content with other users, cannot modify the accounts of other users, and cannot install a content pack from the Marketplace. However, you can import a content pack into your own user space which is visible only to you.
Dashboard User	Dashboard users can only use the Dashboards page of vRealize Log Insight.
View Only Admin	View Admin users can view Admin information, have full User access, and can edit Shared content.
Super Admin	Super Admin users can access the full functionality of vRealize Log Insight, can administer vRealize Log Insight, and can manage the accounts of all other users.

9 Cliquez sur **Enregistrer**.

vRealize Log Insight vérifie que VMware Identity Manager est bien synchronisé avec le groupe spécifié et son domaine. Si le groupe est introuvable, une boîte de dialogue vous informe que vRealize Log Insight ne peut pas vérifier ce groupe. Vous pouvez enregistrer le groupe sans qu'il n'ait été vérifié ou bien annuler pour corriger le nom du groupe ou le domaine.

Les utilisateurs qui appartiennent au groupe que vous avez ajouté peuvent utiliser leur compte VMware Identity Manager pour se connecter à vRealize Log Insight et avoir le même niveau d'autorisation que le groupe auquel ils appartiennent.

Importer un groupe Active Directory dans vRealize Log Insight

Plutôt que d'ajouter des utilisateurs individuels d'un domaine, vous pouvez ajouter des groupes de domaines afin de permettre à des utilisateurs de se connecter à vRealize Log Insight.

When you enable AD support in vRealize Log Insight, you configure a domain name and provide a binding user that belongs to the domain. vRealize Log Insight uses the binding user to verify the connection to the AD domain, and to verify the existence of AD users and groups.


Les groupes Active Directory que vous ajoutez à vRealize Log Insight doivent appartenir au domaine de l'utilisateur de liaison ou à un domaine approuvé par le domaine de l'utilisateur de liaison.

Un utilisateur Active Directory hérite des rôles qui sont attribués à un groupe auquel l'utilisateur appartient, en plus des rôles qui sont attribués à l'utilisateur individuel. Par exemple, un administrateur peut attribuer le rôle **Afficher le compte Admin** au GroupA et attribuer le rôle **Utilisateur** à l'utilisateur Bob. Bob peut également être affecté au GroupA. Lorsque Bob ouvre une session, il hérite du rôle du groupe et dispose des privilèges pour les rôles **Afficher le compte Admin** et **Utilisateur**.

Prérequis

- Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight en tant qu'utilisateur disposant de l'autorisation **Modifier le compte Admin**. Le format de l'URL est `https://log-insight-host` où `log-insight-host` est l'adresse IP ou le nom d'hôte du dispositif virtuel vRealize Log Insight.
- Vérifiez que vous avez configuré la prise en charge d'Active Directory. Reportez-vous à [Permettre l'authentification utilisateur à travers Active Directory](#)

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Access Control**.
- 3 Click **Users and Groups**.
- 4 Sous Groupes de répertoires, cliquez sur **Nouveau groupe**.

5 Cliquez sur Active Directory dans le menu déroulant **Type**.

Le nom de domaine par défaut que vous indiquez lors de la configuration de la prise en charge d'Active Directory s'affiche dans la zone de texte **Domaine**. Si vous ajoutez des groupes du domaine par défaut, ne changez pas le nom de celui-ci.

6 (Facultatif) Si vous souhaitez ajouter un groupe d'un domaine qui approuve le domaine par défaut, tapez le nom du domaine d'approbation dans la zone de texte **Domaine**.

7 Tapez le nom du groupe que vous voulez ajouter.

8 From the **Roles** list on the right, select one or more predefined or custom user roles.

Option	Description
User	Users can access the full functionality of vRealize Log Insight. You can view log events, run queries to search and filter logs, import content packs into their own user space, add alert queries, and manage your own user accounts to change a password or email address. Users do not have access to the administration options, cannot share content with other users, cannot modify the accounts of other users, and cannot install a content pack from the Marketplace. However, you can import a content pack into your own user space which is visible only to you.
Dashboard User	Dashboard users can only use the Dashboards page of vRealize Log Insight.
View Only Admin	View Admin users can view Admin information, have full User access, and can edit Shared content.
Super Admin	Super Admin users can access the full functionality of vRealize Log Insight, can administer vRealize Log Insight, and can manage the accounts of all other users.

9 Cliquez sur **Enregistrer**.

vRealize Log Insight vérifie si le groupe AD existe dans le domaine que vous avez spécifié ou dans un domaine d'approbation. Si le groupe est introuvable, une boîte de dialogue vous informe que vRealize Log Insight ne peut pas vérifier ce groupe. Vous pouvez enregistrer le groupe sans qu'il n'ait été vérifié ou bien annuler pour corriger le nom du groupe.

Les utilisateurs qui appartiennent au groupe Active Directory que vous avez ajouté peuvent utiliser leur compte de domaine pour se connecter à vRealize Log Insight et avoir le même niveau d'autorisation que le groupe auquel ils appartiennent.

Authentification d'utilisateurs avec l'appartenance au groupe inter-domaines

Les administrateurs peuvent autoriser les utilisateurs d'un autre domaine approuvé à s'authentifier pour vRealize Log Insight de deux manières.

- Ajoutez chaque utilisateur manuellement.
- Configurez un groupe dans le même domaine que les utilisateurs et ajoutez le groupe.

Définir un jeu de données


Vous pouvez définir un jeu de données pour permettre à des utilisateurs d'accéder à du contenu spécifique.

Les contraintes de texte ne sont pas compatibles avec les jeux de données.

Prérequis

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Access Control**.
- 3 Click **Data Sets**.
- 4 Cliquez sur **Nouveau jeu de données**.
- 5 Cliquez sur **Ajouter un filtre**.
- 6 Utilisez le premier menu déroulant pour sélectionner un champ défini dans vRealize Log Insight.

Par exemple, **hostname**.

La liste contient tous les champs définis qui sont statistiquement disponibles, en packs de contenu, et sous forme de contenu personnalisé.

Remarque Les champs numériques contiennent les opérateurs supplémentaires =, >, <, >= et <=, que les champs de chaînes ne contiennent pas. Ces opérateurs effectuent des comparaisons numériques. Leur utilisation produit des résultats différents de ceux obtenus avec les opérateurs de chaîne. Par exemple, le filtre **response_time = 02** correspond à un événement contenant un champ **response_time** ayant la valeur 2. Le filtre **response_time contains 02** n'a pas la même correspondance.

- 7 Utilisez le deuxième menu déroulant pour sélectionner l'opération à appliquer au champ sélectionné dans le premier menu déroulant.

Par exemple, sélectionnez **contient**. Le filtre **contains** correspond à des jetons complets : la recherche de la chaîne `err` n'inclut pas `error` dans les résultats obtenus.

- 8 Dans la zone de texte à droite du menu déroulant du filtre, entrez la valeur que vous souhaitez utiliser comme filtre.

Vous pouvez utiliser plusieurs valeurs. L'opérateur logique entre ces valeurs est OU.

Remarque La zone de texte n'est pas disponible si vous sélectionnez l'opérateur **existe** dans le second menu déroulant.

9 (Facultatif) Pour ajouter d'autres filtres, cliquez sur **Ajouter un filtre**.

10 Cliquez **Save**.

Suivant

Associez un jeu de données à un rôle d'utilisateur. Reportez-vous à [Créer et modifier des rôles](#).

Créer et modifier des rôles

Vous pouvez créer des rôles personnalisés ou modifier des rôles prédéfinis afin de permettre aux utilisateurs d'effectuer certaines tâches et d'accéder à des contenus spécifiques.

Prérequis


Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

1 Cliquez le configuration drop-down menu icon  and select **Administration**.

2 Under Management, click **Access Control**.

3 Cliquez **Roles**.

4 Cliquez sur **Nouveau rôle** ou sur  pour modifier un rôle existant.

Vous devez commencer par cloner les rôles Super Admin et Utilisateur avant de pouvoir les modifier.

5 Modifiez les zones de texte **Nom** et **Description**.

6 Sélectionnez une ou plusieurs autorisations dans la liste Autorisations.

Option	Description
Modifier Admin	Permet de modifier les informations et les paramètres Admin.
Afficher Admin	Permet d'afficher les informations et les paramètres Admin.
Modifier partagé	Permet de modifier le contenu partagé.
Analyse	Permet d'utiliser la fonction Analyse interactive.
Tableau de bord	Permet d'afficher les tableaux de bord.

7 (Facultatif) Dans la liste **Jeu de données** de droite, sélectionnez un jeu de données à associer au rôle d'utilisateur.

8 Cliquez **Save**.



Supprimer un compte d'utilisateur à partir de vRealize Log Insight

Vous pouvez supprimer des comptes d'utilisateur en utilisant l'interface utilisateur d'administration de vRealize Log Insight.

Prérequis

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Access Control**.
- 3 Click **Users and Groups**.
- 4 Cochez la case à côté du nom d'utilisateur que vous souhaitez supprimer.
- 5 Cliquez sur l'icône **Supprimer** .

Configuration de l'authentification

3

Vous pouvez utiliser plusieurs méthodes d'authentification avec votre déploiement.

Les méthodes d'authentification incluent l'authentification locale, l'authentification VMware Identity Manager et l'authentification Active Directory. Vous pouvez utiliser plusieurs méthodes dans le même déploiement et les utilisateurs sélectionnent ensuite le type d'authentification à utiliser au moment de la connexion.

vRealize Log Insight inclut une version de vRealize Log Insight disponible sur la page de téléchargement de produit qui comporte l'ensemble des fonctionnalités suivantes :

- Intégration d'annuaire pour authentifier des utilisateurs par rapport à des annuaires existants, tels qu'Active Directory ou LDAP.
- Intégration de l'authentification unique à d'autres produits VMware qui prennent également en charge l'authentification unique
- Authentification unique avec plusieurs fournisseurs d'identité tiers, tels qu'ADFS, Ping Federate, etc.
- Authentification à deux facteurs via l'intégration à un logiciel tiers, tel que RSA SecurID, Entrust, etc. L'authentification à deux facteurs avec VMware Verify n'est pas incluse.

L'authentification locale est un composant de vRealize Log Insight. Pour l'utiliser, vous devez créer un utilisateur local et un mot de passe qui seront stockés sur le serveur vRealize Log Insight.

vRealize Log Insight et Active Directory doivent être activés par un administrateur du produit.

Ce chapitre aborde les rubriques suivantes :

- [Activer l'authentification des utilisateurs via VMware Identity Manager](#)
- [Permettre l'authentification utilisateur à travers Active Directory](#)

Activer l'authentification des utilisateurs via VMware Identity Manager

Lorsqu'elle est activée par un administrateur, l'authentification VMware Identity Manager peut être utilisée avec vRealize Log Insight.


Avec l'authentification VMware Identity Manager, les utilisateurs peuvent utiliser une authentification unique pour tous les produits VMware qui utilisent la même instance d'Identity Manager.

Les utilisateurs d'Active Directory peuvent également être authentifiés via VMware Identity Manager lorsque les serveurs Active Directory et VMware Identity Manager sont synchronisés. Reportez-vous à la documentation VMware Identity Manager pour plus d'informations sur la synchronisation.

Prérequis

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Sous Configuration, cliquez sur **Authentification**.
- 3 Sélectionnez **Activer l'authentification unique**.
- 4 Dans la zone de texte **Hôte**, entrez un identifiant d'hôte pour l'instance de VMware Identity Manager, à utiliser pour l'authentification des utilisateurs.

Par exemple, `company-name.vmwareidentity.com`.
- 5 Dans la zone de texte **Port API**, spécifiez le port à utiliser pour se connecter à l'instance de VMware Identity Manager. La valeur par défaut est 443.
- 6 Vous pouvez éventuellement entrer le nom du locataire VMware Identity Manager. Cette action est obligatoire uniquement si le mode locataire est configuré comme « locataire dans chemin » dans VMware Identity Manager.
- 7 Spécifiez les informations d'identification d'utilisateur de VMware Identity Manager dans les zones de texte **Nom d'utilisateur** et **Mot de passe**.

Ces informations ne sont utilisées qu'une seule fois durant la configuration pour créer un client vRealize Log Insight sur VMware Identity Manager et elles ne sont pas stockées localement dans vRealize Log Insight. L'utilisateur doit disposer des autorisations nécessaires pour exécuter des commandes d'API sur le locataire.
- 8 Cliquez sur **Tester la connexion** pour vérifier que la connexion fonctionne.
- 9 Dans le menu déroulant **URL de redirection de l'hôte**, sélectionnez le nom d'hôte ou l'adresse IP à utiliser dans l'URL de redirection pour l'enregistrement sur VMware Identity Manager.

Si au moins une adresse IP virtuelle est définie pour l'équilibrage de charge intégré, VMware Identity Manager redirige l'adresse IP virtuelle sélectionnée. Si l'équilibrage de charge intégré n'est pas configuré, l'adresse IP du nœud maître est utilisée à la place.
- 10 Choisissez d'autoriser ou non la prise en charge des connexions des utilisateurs Active Directory via VMware Identity Manager.

Cette option peut être utilisée pour les utilisateurs Active Directory lorsque VMware Identity Manager est synchronisé avec cette instance d'Active Directory.
- 11 Click **Save**.


Permettre l'authentification utilisateur à travers Active Directory

Vous pouvez authentifier les utilisateurs par le biais d'Active Directory. Cela simplifie le journal en cours de traitement pour les utilisateurs en leur permettant d'utiliser un mot de passe commun à plusieurs fins.

Prérequis

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Sous Configuration, cliquez sur **Authentification**.
- 3 Sélectionnez **Activer la prise en charge d'Active Directory**.
- 4 Dans la zone de texte **Domaine par défaut**, tapez un nom de domaine.

Par exemple, **company-name.com**.

Remarque Vous ne pouvez pas indiquer plusieurs domaines dans la zone de texte Domaine par défaut. Si le domaine par défaut que vous indiquez est approuvé par d'autres domaines, vRealize Log Insight utilise le domaine par défaut et l'utilisateur de liaison pour vérifier les utilisateurs et les groupes AD dans les domaines d'approbation.

Si vous basculez vers un autre domaine incluant déjà des utilisateurs et des groupes, l'authentification échouera pour les utilisateurs et les groupes existants, et les données enregistrées par les utilisateurs existants seront perdues.

- 5 Si vous disposez de contrôleurs de domaine géolocalisés ou dont la sécurité est limitée, spécifiez manuellement les contrôleurs de domaine les plus proches de cette instance de vRealize Log Insight.

Remarque Les serveurs d'autorisation Active Directory équilibrés en charge ne sont pas pris en charge.

- 6 Entrez les informations d'identification d'un utilisateur de liaison appartenant au domaine par défaut. vRealize Log Insight utilise le domaine par défaut et l'utilisateur de liaison pour vérifier les utilisateurs et les groupes AD dans le domaine par défaut et dans les domaines qui approuvent ce dernier.
- 7 Spécifiez des valeurs pour le type de connexion.
Cette connexion est utilisée pour l'authentification Active Directory.
- 8 Click **Save**.

Suivant

Accordez aux utilisateurs et aux groupes AD les autorisations requises pour accéder à l'instance actuelle de vRealize Log Insight.

Configurer le protocole à utiliser pour Active Directory

Vous pouvez configurer le protocole à utiliser lors de la connexion à Active Directory. Par défaut, vRealize Log Insight tente d'abord de se connecter à Active Directory en utilisant le protocole LDAP avec SSL puis, si besoin, en utilisant le protocole LDAP sans SSL.

Si vous souhaitez utiliser un seul protocole pour la communication Active Directory ou si vous souhaitez modifier l'ordre dans lequel les protocoles sont utilisés, vous devez appliquer des configurations supplémentaires au dispositif virtuel vRealize Log Insight.

Prérequis

- Vérifiez que vous disposez des informations d'identification de l'utilisateur racine pour vous connecter au dispositif virtuel vRealize Log Insight. Reportez-vous à [Configurer le mot de passe SSH racine du dispositif virtuel vRealize Log Insight](#)
- Pour activer les connexions SSH, vérifiez que le port TCP 22 est ouvert.

Procédure

- 1 Établissez une connexion SSH au dispositif virtuel vRealize Log Insight, puis connectez-vous en tant qu'utilisateur racine.
- 2 Accédez à l'emplacement suivant : `/storage/var/loginsight/config`
- 3 Localisez le fichier de configuration le plus récent pour lequel le [nombre] est le plus grand : `/storage/core/loginsight/config/loginsight-config.xml#[number]`
- 4 Copiez le fichier de configuration le plus récent : `/storage/core/loginsight/config/loginsight-config.xml#[number]`
- 5 Augmentez le [nombre] et enregistrez-le à l'emplacement suivant : `/storage/core/loginsight/config/loginsight-config.xml#[number + 1]`
- 6 Ouvrez le fichier pour le modification.
- 7 Dans la section Authentication, ajoutez la ligne correspondant à la configuration que vous souhaitez appliquer :

Option	Description
<code><ad-protocols value="LDAP" /></code>	Pour utiliser LDAP sans SSL
<code><ad-protocols value="LDAPS" /></code>	Pour utiliser uniquement LDAP avec SSL

Option	Description
<code><ad-protocols value="LDAP, LDAPS" /></code>	Pour utiliser LDAP en premier lieu, puis LDAP avec SSL en second lieu
<code><ad-protocols value="LDAPS, LDAP" /></code>	Pour utiliser LDAP en premier lieu, puis LDAP sans SSL en second lieu

Si vous ne sélectionnez aucun protocole, vRealize Log Insight tente d'abord d'utiliser LDAP, puis LDAP avec SSL.

- 8 Enregistrez et fermez le fichier.
- 9 Exécutez la commande `service loginsight restart`.

Configuration de vRealize Log Insight

4

Vous pouvez configurer et personnaliser vRealize Log Insight pour modifier les paramètres par défaut, les paramètres réseau et les ressources de stockage. Vous pouvez également configurer des notifications système.

Ce chapitre aborde les rubriques suivantes :

- [Limites de configuration de vRealize Log Insight](#)
- [Configuration des paramètres du dispositif virtuel](#)
- [Attribuer une licence permanente à vRealize Log Insight](#)
- [Stratégie de stockage des journaux](#)
- [Gestion des notifications système](#)
- [Ajouter une destination de transfert d'événements de vRealize Log Insight](#)
- [Synchroniser l'heure sur le dispositif virtuel vRealize Log Insight](#)
- [Configurer le serveur SMTP pour vRealize Log Insight](#)
- [Installer un certificat SSL personnalisé](#)
- [Modifier le délai d'expiration par défaut des sessions Web de vRealize Log Insight](#)
- [Archives](#)
- [Redémarrer le service vRealize Log Insight](#)
- [Mettre le dispositif virtuel vRealize Log Insight hors tension](#)
- [Télécharger un bundle de support vRealize Log Insight](#)
- [Rejoindre ou quitter le programme d'amélioration du produit VMware](#)

Limites de configuration de vRealize Log Insight

Lorsque vous configurez vRealize Log Insight, vous devez rester en dessous ou au niveau des valeurs maximales prises en charge.

Tableau 4-1. Configurations maximales de vRealize Log Insight

Élément	Maximum
Configuration de nœuds	
CPU	16 vCPU
Mémoire	32 Go
Périphérique de stockage (vmdk)	2 To - 512 octets
Stockage adressable total	4 To (+ lecteur du système d'exploitation) Un stockage de journal adressable de 4 To au maximum sur des VMDK avec une taille maximale de 2 To chacun. Vous pouvez disposer de deux VMDK de 2 To ou de quatre VMDK de 1 To, etc. Lorsque vous atteignez la valeur maximale, vous devrez agrandir l'échelle avec une taille de cluster supérieure au lieu d'ajouter des disques aux machines virtuelles existantes.
Connexions Syslog	750
Configuration de clusters	
Nœuds	12 (maître + 11 travailleurs)
Ingestion par nœud	
Événements par seconde	15 000 eps
Longueur du message Syslog	10 Ko (champ de texte)
Demande API Ingestion HTTP POST	16 Ko (champ texte) ; 4 Mo par demande HTTP POST
Intégrations	
vRealize Operations Manager	1
vSphere vCenter Server	10
Domaines Active Directory	1
Serveurs de messagerie	1
Serveurs DNS	2
Serveurs NTP	4
Redirecteurs	10

Configuration des paramètres du dispositif virtuel

Vous pouvez modifier les paramètres du dispositif virtuel, notamment la capacité de stockage et de mémoire ou la capacité du CPU.

Configurer le mot de passe SSH racine du dispositif virtuel vRealize Log Insight

Par défaut, la connexion SSH au dispositif virtuel est désactivée. Vous pouvez configurer le mot de passe SSH racine à partir de VMware Remote Console ou lorsque vous déployez le dispositif virtuel vRealize Log Insight.

Il vous est recommandé de définir le mot de passe SSH racine lorsque vous déployez le fichier .ova de vRealize Log Insight. Pour plus d'informations, consultez [Déployer le dispositif virtuel vRealize Log Insight](#).

Vous pouvez également activer SSH et définir le mot de passe racine à partir de VMware Remote Console.

Prérequis

Vérifiez que le dispositif virtuel vRealize Log Insight est déployé et en cours d'exécution.

Procédure

- 1 Dans l'inventaire vSphere Client, cliquez sur le dispositif virtuel vRealize Log Insight, puis ouvrez l'onglet **Console**.
- 2 Accédez à une ligne de commande en utilisant la combinaison de touches indiquée sur l'écran de démarrage.
- 3 Dans la console, tapez **root**, puis appuyez sur la touche Entrée. Laissez le champ du mot de passe vide, puis appuyez sur la touche Entrée.

La console affiche le message suivant : Le mot de passe doit être changé. Choisissez un nouveau mot de passe.

- 4 Laissez le champ de l'ancien mot de passe vide, puis appuyez sur la touche Entrée.
- 5 Tapez le nouveau mot de passe de l'utilisateur racine, appuyez sur la touche Entrée, tapez une deuxième fois le nouveau mot de passe de l'utilisateur racine, puis appuyez de nouveau sur la touche Entrée.

Le mot de passe doit être composé d'un minimum de 8 caractères et doit inclure au moins une majuscule, une minuscule, un chiffre et un caractère spécial. Le même caractère ne doit pas être répété plus de quatre fois.

Le message suivant s'affiche : Mot de passe modifié.

Suivant

Le mot de passe racine ne peut pas être utilisé pour établir des connexions SSH au dispositif virtuel vRealize Log Insight.

Modifier les paramètres réseau du vApp vRealize Log Insight

Vous pouvez modifier les paramètres réseau du dispositif virtuel de vRealize Log Insight en modifiant les propriétés du vApp dans vSphere Client.

Prérequis

Vérifiez que vous disposez des autorisations requises pour modifier les propriétés du vApp.

Procédure

- 1 Mettez le vApp vRealize Log Insight hors tension.
- 2 Cliquez avec le bouton droit sur le vApp vRealize Log Insight dans l'inventaire, puis cliquez sur **Modifier les paramètres**.
- 3 Cliquez sur l'onglet **Options**, puis sélectionnez **Options vApp > Stratégie d'allocation d'adresses IP**.
- 4 Sélectionnez une option d'allocation d'IP.

Option	Description
Fixe	Les adresses IP sont configurées manuellement. Aucune allocation automatique n'est effectuée.
Transitoire	Les adresses IP sont allouées automatiquement grâce aux pools IP provenant d'une plage spécifiée quand le vApp est sous tension. Les adresses IP sont libérées quand le dispositif est mis hors tension.
DHCP	Un serveur DHCP est utilisé pour allouer les adresses IP. Les adresses assignées par le serveur DHCP sont visibles dans les environnements OVF des machines virtuelles démarrées dans le vApp.

- 5 (Facultatif) Si vous sélectionnez **Fixe**, cliquez sur **Options vApp > Propriétés** et attribuez une adresse IP, un masque réseau, une passerelle, un nom d'hôte et un DNS pour le vApp de vRealize Log Insight.

Avertissement N'indiquez pas plus de deux serveurs de noms de domaine. Si vous en indiquez plus de deux, le dispositif virtuel vRealize Log Insight ignore tous les serveurs de noms de domaine configurés.

- 6 Mettez le vApp vRealize Log Insight sous tension.

Augmenter la capacité de stockage du dispositif virtuel vRealize Log Insight

Vous pouvez augmenter les ressources de stockage allouées à vRealize Log Insight à mesure que vos besoins évoluent.

Augmentez l'espace de stockage en ajoutant un nouveau disque virtuel au dispositif virtuel vRealize Log Insight. Vous pouvez ajouter autant de disques que nécessaire, jusqu'à 4 To (+ lecteur du système d'exploitation) de stockage adressable total. Le total peut être une combinaison de deux disques de 2 To ou de quatre disques de 1 To et ainsi de suite. Reportez-vous à [Limites de configuration de vRealize Log Insight](#).

Prérequis

- Log in to the vSphere Client as a user who has privileges to modify the hardware of virtual machines in the environment.
- Arrêtez le dispositif virtuel vRealize Log Insight en toute sécurité. Reportez-vous à [Mettre le dispositif virtuel vRealize Log Insight hors tension](#)

Procédure

- 1 In the vSphere Client inventory, right-click the vRealize Log Insight virtual machine and select **Edit Settings**.
- 2 On the **Hardware** tab, click **Add**.
- 3 Sélectionnez **Disque dur** et cliquez sur **Suivant**.

4 Sélectionnez **Créer un disque virtuel** et cliquez sur **Suivant**.

a Indiquez la capacité du disque.

vRealize Log Insight prend en charge les disques durs virtuels jusqu'à 2 To. Si vous avez besoin d'une capacité supérieure, ajoutez plusieurs disques durs virtuels.

b Sélectionnez un format de disque.

Option	Description
Provisionnement statique mis à zéro en différé	Crée un disque virtuel au format statique par défaut. L'espace nécessaire pour le disque virtuel est alloué lorsque le disque virtuel est créé. Les données résidant sur le périphérique physique ne sont pas effacées lors de la création. Elles sont mises à zéro ultérieurement à la demande, après la première écriture effectuée par la machine virtuelle.
Provisionnement statique immédiatement mis à zéro	Crée un type de disque virtuel statique qui prend en charge des fonctions telles que Fault Tolerance. L'espace nécessaire au disque virtuel est alloué lors de la création. Contrairement au format plat, les données qui résident sur le périphérique physique sont mises à zéro lors de la création du disque virtuel. La création de disques dans ce format peut être plus longue que pour d'autres types de disques. Autant que possible, créez des disques à provisionnement statique immédiatement mis à zéro pour obtenir de meilleures performances et un fonctionnement optimal du dispositif virtuel vRealize Log Insight.
Thin Provision	Crée un disque dans le format léger. Employez ce format pour économiser de l'espace de stockage.

c Pour sélectionner une banque de données, accédez à son emplacement et cliquez sur **Suivant**.

5 Acceptez le nœud du périphérique virtuel par défaut et cliquez sur **Suivant**.

6 Review the information and click **Finish**.

7 Click **OK** to save your changes and close the dialog box.

Lorsque vous mettez le dispositif virtuel vRealize Log Insight sous tension, la machine virtuelle détecte le nouveau disque virtuel et l'ajoute automatiquement au volume de données par défaut. Mettez d'abord la machine virtuelle complètement hors tension. Pour plus d'informations sur la mise sous tension des dispositifs virtuels, consultez <https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-6-pubs.html>.

Avertissement Après avoir ajouté un disque au dispositif virtuel, vous ne pouvez plus le retirer en toute sécurité. Le retrait de disques du dispositif virtuel vRealize Log Insight peut provoquer la perte complète des données.

Ajouter de la mémoire et des CPU au dispositif virtuel vRealize Log Insight

Après le déploiement, vous pouvez modifier la quantité de mémoire et le nombre de CPU alloués à un dispositif virtuel vRealize Log Insight.

Vous pouvez être amené à modifier l'allocation des ressources (par exemple, si le nombre d'événements dans votre environnement augmente).

Prérequis

- Connectez-vous à vSphere Client en tant qu'utilisateur disposant des privilèges requis pour modifier le matériel des machines virtuelles dans l'environnement.
- Arrêtez le dispositif virtuel vRealize Log Insight en toute sécurité. Reportez-vous à [Mettre le dispositif virtuel vRealize Log Insight hors tension](#)

Procédure

- 1 In the vSphere Client inventory, right-click the vRealize Log Insight virtual machine and select **Edit Settings**.
- 2 On the **Hardware** tab, click **Add**.
- 3 Vous pouvez ajuster le nombre de CPU et la quantité de mémoire à votre guise.
- 4 Review the information and click **Finish**.
- 5 Click **OK** to save your changes and close the dialog box.

Au moment où vous mettez le dispositif virtuel vRealize Log Insight sous tension, la machine virtuelle commence à utiliser les nouvelles ressources.

Attribuer une licence permanente à vRealize Log Insight

Vous pouvez utiliser vRealize Log Insight uniquement si vous disposez d'une clé de licence valide.

Lorsque vous téléchargez vRealize Log Insightsur le site Web de VMware, vous obtenez une licence d'évaluation qui est valide pendant 60 jours. Une fois que la licence d'évaluation a expiré, vous devez attribuer une licence permanente à vRealize Log Insight pour pouvoir continuer à l'utiliser.

Dans le cadre de l'interopérabilité entre solutions, les utilisateurs de VMware NSX des éditions Standard, Advanced ou Enterprise peuvent attribuer une licence à vRealize Log Insight avec leur clé de licence NSX. Pour plus d'informations, consultez la documentation de VMware NSX.


Utilisez la section Administration de l'interface utilisateur Web de vRealize Log Insight pour vérifier l'état de la licence de vRealize Log Insight et la gérer.

Prérequis

- Obtenez une clé de licence valide sur My VMware™.

- Verify that you are logged in to the vRealize Log Insight *portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Sous Gestion, sélectionnez **Licence**.
- 3 Dans la zone de texte **Clé de licence**, tapez votre clé de licence, puis cliquez sur **Définir la clé**. Si vous disposez d'une clé de licence VMware NSX, entrez-la ici.
- 4 Vérifiez que l'état de la licence est Actif, et que le type de licence et sa date d'expiration sont corrects.

Stratégie de stockage des journaux

Le dispositif virtuel vRealize Log Insight utilise au moins 100 Go de stockage pour les journaux entrants.

Lorsque le volume des journaux importés dans vRealize Log Insight atteint la limite de 100 Go, les anciens messages de journaux sont retirés de manière automatique et régulière. Les plus anciens sont retirés en premier. Pour conserver les anciens messages, activez la fonctionnalité d'archivage de vRealize Log Insight. Reportez-vous à [Activer ou désactiver l'archivage des données dans vRealize Log Insight](#).

Les données stockées par vRealize Log Insight ne sont pas modifiables. Une fois un journal importé, il ne peut pas être supprimé, à moins d'être retiré de manière automatique.

Gestion des notifications système

vRealize Log Insight comporte un dispositif intégré de notifications système concernant l'activité liée à la santé de vRealize Log Insight. Il signale par exemple que l'espace disque est presque épuisé ou que les anciens fichiers journaux sont sur le point d'être supprimés. Les administrateurs peuvent configurer à quel endroit envoyer ces notifications système et à quelle fréquence.

Les notifications système vous indiquent les problèmes critiques qui nécessitent une attention immédiate, vous envoient des avertissements qui peuvent exiger une réponse et vous informent de l'état de l'activité normale du système. Les notifications système sont interrompues pendant les mises à niveau, mais sont effectives tout le reste du temps.

Un administrateur peut spécifier la fréquence à laquelle les notifications sont envoyées et à quelles adresses e-mails. Les notifications système concernant vRealize Log Insight peuvent également être envoyées à des applications tierces.

Les notifications système sont différentes des requêtes d'alerte, ces dernières étant définies par l'utilisateur. Pour plus d'informations sur les requêtes d'alerte, consultez [Ajouter une requête d'alerte à Log Insight pour l'envoi de notifications par e-mail](#).

Notifications système dans vRealize Log Insight

vRealize Log Insight propose deux ensembles de notifications, les notifications générales, applicables à toutes les configurations de produit, et les notifications relatives aux clusters pour les déploiements basés sur un cluster.

Les tableaux suivants répertorient et décrivent les notifications système dans vRealize Log Insight.

Notifications système générales

vRealize Log Insight envoie des notifications lorsqu'une situation peut nécessiter l'intervention de l'administrateur, notamment en cas d'échec de l'archivage ou de retards dans la planification des alertes.

Nom de la notification	Description
Vous ne pourrez bientôt plus rechercher les données les plus anciennes	<p>Cette notification vous informe du moment où vRealize Log Insight va commencer à désaffecter les anciennes données de l'espace de stockage du dispositif virtuel et vous indique la taille attendue des données pouvant être recherchées selon le taux d'ingestion actuel. Si vous avez configuré l'archivage, les données ayant changé sont archivées ; sinon, elles sont supprimées.</p> <p>La notification est envoyée après chaque redémarrage du service vRealize Log Insight.</p>
Durée de rétention du référentiel	<p>Une période de rétention correspond à la durée pendant laquelle les données sont conservées sur le disque local de votre instance vRealize Log Insight. Une période de rétention est déterminée par le volume de données que le système peut contenir et le taux d'ingestion actuel. Par exemple, si vous recevez 10 Go/jour de données (après indexation) et que vous disposez de 300 Go d'espace, votre taux de rétention est de 30 jours. Lorsque la limite de stockage est atteinte, les anciennes données sont supprimées pour laisser de l'espace aux données venant d'être ingérées.</p> <p>Cette notification vous indique lorsque le volume de données pouvant être recherchées et que vRealize Log Insight peut stocker, en fonction du taux d'ingestion actuel, dépasse l'espace de stockage disponible sur le dispositif virtuel.</p> <p>Les utilisateurs Admin peuvent définir le seuil de notification relatif au stockage. Reportez-vous à Configurer vRealize Log Insight pour envoyer des notifications de santé.</p>

Nom de la notification	Description
Événements annulés	<p>Cette notification vous indique que vRealize Log Insight n'a pas réussi à ingérer tous les messages de journaux entrants.</p> <ul style="list-style-type: none"> ■ En cas d'annulation de messages TCP, selon le suivi effectué par le serveur de vRealize Log Insight, une notification système est envoyée dans les deux cas suivants : <ul style="list-style-type: none"> ■ Une fois par jour ■ Chaque fois que le service vRealize Log Insight est redémarré (manuellement ou automatiquement). ■ L'e-mail contient le nombre de messages ayant été annulés depuis l'envoi de la dernière notification par e-mail et le nombre total d'annulations de messages depuis le dernier redémarrage de vRealize Log Insight. <p>Remarque L'heure indiquée sur la ligne d'envoi dépend du client de messagerie et suit le fuseau horaire local, alors que le corps de texte de l'e-mail indique l'heure UTC.</p>
Compartiments d'index corrompus	<p>Cette notification vous informe qu'une partie de l'index sur disque est corrompue, ce qui indique en général de graves problèmes au niveau du système de stockage sous-jacent. La partie corrompue de l'index est exclue des requêtes de service. Un index corrompu a une incidence sur l'ingestion des nouvelles données. vRealize Log Insight vérifie l'intégrité de l'index après le démarrage du service. Si une corruption de l'index est détectée, vRealize Log Insight envoie une notification système dans les deux cas suivants :</p> <ul style="list-style-type: none"> ■ Une fois par jour ■ Chaque fois que le service vRealize Log Insight est redémarré (manuellement ou automatiquement).
Disque insuffisant	<p>Cette notification vous indique que l'espace disque de vRealize Log Insight est en train de s'épuiser. Elle vous informe que vRealize Log Insight subit probablement un problème de stockage.</p>

Nom de la notification	Description
L'espace d'archivage va être plein	Cette notification vous indique que l'espace disque utilisé pour l'archivage des données vRealize Log Insight sur le serveur NFS sera bientôt épuisé.
Modification de l'espace disque total	<p>Cette notification vous informe que la taille totale de la partition destinée au stockage des données vRealize Log Insight a diminué, ce qui indique en général une erreur grave du système de stockage sous-jacent. Lorsque vRealize Log Insight détecte cette condition, la notification est envoyée comme suit :</p> <ul style="list-style-type: none"> ■ Immédiatement ■ Une fois par jour
Archivages en attente	Cette notification vous informe que vRealize Log Insight ne peut pas archiver les données comme prévu, ce qui indique en général des problèmes au niveau du stockage NFS que vous avez configuré pour l'archivage des données.
La licence est sur le point d'expirer	Cette notification vous indique que la licence de vRealize Log Insight est sur le point d'expirer.
La licence a expiré	Cette notification vous indique que la licence de vRealize Log Insight a expiré.
Connexion au serveur AD impossible	Cette notification vous informe que vRealize Log Insight ne parvient pas à se connecter au serveur Active Directory configuré.

Nom de la notification	Description
Impossible de récupérer l'adresse IP High Availability [adresse IP], car elle est déjà prise par une autre machine	<p>Cette notification vous avertit que le cluster vRealize Log Insight n'a pas pu récupérer l'adresse IP configurée pour l'équilibrage de charge intégré (ILB). Cette notification se produit le plus souvent lorsqu'un autre hôte du même réseau détient l'adresse IP et que celle-ci ne peut donc pas être prise par le cluster.</p> <p>Vous pouvez résoudre ce conflit en libérant l'adresse IP de l'hôte qui la détient actuellement ou en configurant l'équilibrage de charge intégrée de Log Insight avec une adresse IP statique disponible sur le réseau. Lors de la modification de l'adresse IP d'ILB, n'oubliez pas de configurer tous les clients pour envoyer tous les journaux à la nouvelle adresse IP ou à un nom de domaine complet/URL dont la résolution correspond à cette adresse IP. Vous devez également annuler la configuration de chaque système vCenter Server intégré avec vRealize Log Insight, puis le reconfigurer à partir de la page Intégration vSphere.</p>

Nom de la notification	Description
L'adresse IP High Availability [adresse IP] n'est pas disponible en raison d'un trop grand nombre de pannes de nœuds	<p>Cette notification vous avertit que l'adresse IP configurée pour l'équilibrage de charge intégré (ILB) n'est pas disponible. Cela signifie que les clients qui tentent d'envoyer des journaux à un cluster vRealize Log Insight via l'adresse IP ILB ou via un nom de domaine complet/URL dont la résolution équivaut à cette adresse IP, verront cette adresse comme non disponible. Cette notification se produit le plus souvent lorsqu'une majorité des nœuds du cluster vRealize Log Insight sont défectueux ou inaccessibles à partir du nœud maître. Elle peut également se produire lorsque la synchronisation de l'heure NTP n'a pas été activée ou que les serveurs NTP configurés présentent entre eux un décalage horaire significatif. Vous pouvez confirmer que le problème persiste en essayant d'exécuter une commande ping (si elle est autorisée) sur une adresse IP pour vérifier son accessibilité.</p> <p>Pour résoudre ce problème, vérifiez l'intégrité et la disponibilité de la plupart de vos nœuds de clusters et activez la synchronisation de l'heure NTP sur des serveurs NTP précis.</p>
Trop de migrations de l'adresse IP High Availability [votre adresse IP] entre nœuds vRealize Log Insight	<p>Cette notification vous avertit que l'adresse IP configurée pour l'équilibrage de charge intégré (ILB) a migré trop souvent au cours des 10 dernières minutes. Dans des conditions de fonctionnement normales, l'adresse IP se déplace rarement entre les nœuds de cluster vRealize Log Insight. Cependant, l'adresse IP peut se déplacer si le nœud propriétaire actuel redémarre ou passe en mode de maintenance. Il se peut également que la synchronisation de l'heure ne soit pas activée entre des nœuds de clusters Log Insight, synchronisation essentielle pour garantir le bon fonctionnement des clusters. Dans ce dernier cas, vous pouvez corriger le problème en activant la synchronisation de l'heure NTP sur des serveurs NTP précis.</p>

Nom de la notification	Description
Erreur de certificat SSL	<p>Cette notification vous informe qu'une source Syslog a lancé une connexion à vRealize Log Insight via SSL, mais qu'elle a brusquement mis fin à la connexion. Cela peut indiquer que la source Syslog n'a pas pu confirmer la validité du certificat SSL. Pour permettre à vRealize Log Insight d'accepter des messages syslog sur SSL, un certificat validé par le client est requis et les horloges des systèmes doivent être synchronisées. Le certificat SSL ou le service de temps du réseau peut présenter un problème.</p> <p>Vous pouvez valider que le certificat SSL est approuvé par votre source Syslog, reconfigurer la source pour ne pas utiliser SSL ou réinstaller le certificat SSL. Reportez-vous à la section Configurer les paramètres SSL de l'agent vRealize Log Insight et à la section Installer un certificat SSL personnalisé.</p>
La collecte vCenter a échoué	<p>Cette notification vous informe que vRealize Log Insight ne peut pas collecter d'événements, de tâches et d'alarmes vCenter. Pour rechercher l'erreur exacte à l'origine de l'échec de la collecte et pour vérifier si la collecte est en cours d'exécution, reportez-vous au fichier <code>/storage/var/loginsight/plugins/vsphere/li-vsphere.log</code>.</p>
Événements abandonnés par le redirecteur d'événements	<p>Cette notification système est envoyée lorsqu'un redirecteur d'événements abandonne des événements en raison de problèmes de connexion ou de surcharge.</p> <p>Exemple :</p> <pre data-bbox="1021 1428 1425 1816">Log Insight Admin Alert: Event Forwarder Events Dropped This alert is about your Log Insight installation on https://<your_url> Event Forwarder Events Dropped triggered at 2016-08-02T18:41:06.972Z Log Insight just dropped 670 events for forwarder target 'Test', reason: Pending queue is full.</pre>

	Nom de la notification	Description
	Requêtes d'alertes derrière la planification	Cette notification vous informe que vRealize Log Insight n'a pas pu exécuter une alerte utilisateur à l'heure configurée. Le retard peut être dû à une ou plusieurs alertes utilisateur inefficaces ou à une taille inadéquate du système pour la charge d'ingestion et de requête.
	Alerte désactivée automatiquement	Si une alerte a été exécutée au moins dix fois et que sa durée moyenne d'exécution est supérieure à une heure, l'alerte est jugée inefficace et elle est désactivée pour éviter d'affecter les autres alertes utilisateur.
	Requête d'alerte inefficace	Si l'exécution d'une alerte dure plus d'une heure, l'alerte est jugée inefficace.

Notifications système pour les clusters

vRealize Log Insight envoie des notifications concernant les modifications de topologie des clusters, notamment l'ajout de nouveaux membres au cluster ou les problèmes de communication temporaires des nœuds.

Expéditeur	Nom de la notification	Description
Nœud maître	Un nouveau nœud travailleur nécessite une approbation	Cette notification vous indique qu'un nœud travailleur a fait une demande d'appartenance. Un utilisateur Admin doit approuver la demande ou la rejeter.
Nœud maître	Un nouveau nœud travailleur a été approuvé	Cette notification vous indique qu'un utilisateur Admin a approuvé la demande d'appartenance d'un nœud travailleur souhaitant rejoindre un cluster vRealize Log Insight.
Nœud maître	Un nouveau nœud travailleur a été refusé	Cette notification vous indique qu'un utilisateur Admin a rejeté la demande d'appartenance d'un nœud travailleur souhaitant rejoindre un cluster vRealize Log Insight. Si la demande a été refusée par erreur, un utilisateur Admin peut envoyer de nouveau la demande depuis le travailleur, puis l'approuver dans le nœud maître.
Nœud maître	Le nombre maximal de nœuds pris en charge a été dépassé à cause du nœud travailleur	Cette notification vous indique que le nombre de nœuds travailleurs du cluster Log Insight est supérieur au nombre maximal pris en charge en raison de la présence d'un nouveau nœud travailleur.

Expéditeur	Nom de la notification	Description
Nœud maître	Le nombre de nœuds autorisés a été dépassé et le nouveau nœud travailleur est refusé	Cette notification vous indique qu'un utilisateur Admin a tenté d'ajouter au cluster davantage de nœuds que le nombre maximal autorisé et que l'ajout du nœud a été refusé.
Nœud maître	Nœud travailleur déconnecté	Cette notification vous indique qu'un nœud travailleur connecté au cluster vRealize Log Insight s'est déconnecté.
Nœud maître	Nœud travailleur reconnecté	Cette notification vous indique qu'un nœud travailleur s'est reconnecté au cluster vRealize Log Insight.
Nœud maître	Nœud travailleur révoqué par l'administrateur	Cette notification vous indique qu'un utilisateur Admin a révoqué l'appartenance d'un nœud travailleur et que ce dernier ne fait plus partie du cluster vRealize Log Insight.
Nœud maître	Nœud travailleur inconnu rejeté	Cette notification vous indique que le nœud maître vRealize Log Insight a rejeté la demande d'un nœud travailleur, car il lui est inconnu. Si le nœud travailleur est valide et qu'il doit être ajouté au cluster, connectez-vous au nœud travailleur, supprimez son fichier de jeton et la configuration utilisateur à l'emplacement /storage/core/loginsight/config/, puis exécutez <code>restart loginsight service</code> sur le nœud travailleur.
Nœud maître	Le nœud travailleur est passé en mode de maintenance	Cette notification vous indique qu'un nœud travailleur est passé en mode de maintenance. Pour pouvoir modifier la configuration et pour que le nœud travailleur puisse servir des requêtes, un utilisateur Admin doit désactiver ce mode sur le nœud.
Nœud maître	Le nœud travailleur est revenu en mode service	Cette notification vous indique qu'un nœud travailleur n'est plus en mode de maintenance et qu'il est revenu en mode service.

Expéditeur	Nom de la notification	Description
Nœud travailleur	Le maître a échoué ou s'est déconnecté du nœud travailleur	<p>Cette notification vous indique que le nœud travailleur qui envoie la notification ne peut pas contacter le nœud maître vRealize Log Insight. Cela peut indiquer que le nœud maître a échoué et qu'un redémarrage de ce dernier est nécessaire. En cas d'échec du nœud maître, le cluster ne peut pas être configuré et les requêtes ne peuvent pas être envoyées jusqu'à ce que le nœud soit de nouveau en ligne. Les nœuds travailleurs continuent cependant à ingérer des messages.</p> <p>Remarque Il peut vous arriver de recevoir plusieurs notifications de ce genre, car plusieurs nœuds travailleurs peuvent détecter la panne du nœud maître et envoyer chacun une notification.</p>
Nœud travailleur	Nœud maître connecté au nœud travailleur	Cette notification vous indique que le nœud travailleur qui envoie la notification est reconnecté au nœud maître vRealize Log Insight.

Configuration de notifications système vRealize Log Insight

En tant qu'administrateur, vous pouvez configurer des notifications système vRealize Log Insight pour envoyer des notifications système à des applications tierces et envoyer un e-mail à des utilisateurs spécifiés lorsqu'une notification est déclenchée.

vRealize Log Insight génère ces notifications lorsqu'un important événement système a lieu (par exemple, lorsque l'espace disque est presque épuisé et que vRealize Log Insight doit commencer à supprimer ou à archiver les fichiers journaux anciens).

Configurer vRealize Log Insight pour envoyer des notifications de santé


Un administrateur peut configurer vRealize Log Insight de manière à envoyer des notifications relatives à la santé de l'application.

Si un message électronique ne peut pas être remis, vous êtes averti de l'erreur sur l'interface Web.

Prérequis

- Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.
- Vérifiez que le serveur SMTP est configuré pour vRealize Log Insight. Pour plus d'informations, consultez [Configurer le serveur SMTP pour vRealize Log Insight](#).

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Configuration, click **General**.
- 3 Sous l'en-tête Alertes, configurez les notifications système.
 - a Dans la zone de texte **Envoyer les notifications système par e-mail à**, tapez les adresses e-mail auxquelles les notifications doivent être envoyées.
Utilisez des virgules pour séparer les différentes adresses e-mail, le cas échéant.
 - b Cochez la case **Seuil des notifications de rétention** et définissez le seuil qui déclenche les notifications.
Une notification est envoyée lorsque la quantité de données que le système peut contenir est insuffisante pour la période spécifiée. Cette valeur est calculée en fonction du taux d'ingestion actuel.
- 4 Click **Save**.
- 5 Click **Restart Log Insight** to apply your changes.

Configurer des notifications système de vRealize Log Insight pour des produits tiers


Un administrateur peut configurer vRealize Log Insight de manière à envoyer des notifications relatives à la santé de l'application à des applications tierces.

vRealize Log Insight génère ces notifications lorsqu'un important événement système a lieu (par exemple, lorsque l'espace disque est presque épuisé et que vRealize Log Insight doit commencer à supprimer les fichiers journaux anciens).

Prérequis

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Configuration, click **General**.
- 3 Sous l'en-tête Alertes, configurez les notifications système.
 - a Dans la zone de texte **Envoyer des notifications système HTTP Post à**, tapez les URL auxquelles les notifications doivent être envoyées.
 - b (Facultatif) Vérifiez que la case **Envoyer une notification lorsque la capacité descend au-dessous de** et le seuil associé sont configurés correctement pour votre environnement.
- 4 Click **Save**.

Suivant

En utilisant la sortie de webhook pour votre notification, créez un shim pour mapper le format de webhook de vRealize Log Insight au format utilisé par votre application tierce.

À propos de l'utilisation de webhooks pour envoyer des notifications système à des produits tiers

Vous pouvez envoyer des notifications système vRealize Log Insight à des produits tiers en utilisant des webhooks.

vRealize Log Insight utilise des webhooks pour envoyer des alertes sur HTTP POST à d'autres applications. vRealize Log Insight envoie un webhook dans son propre format propriétaire, mais les solutions tierces attendent des webhooks entrants dans leur propre format propriétaire. Pour utiliser les informations envoyées avec des webhooks vRealize Log Insight, l'application tierce doit prendre en charge nativement le format de vRealize Log Insight ou vous devez créer un mappage entre les formats de vRealize Log Insight et le format utilisé par le produit tiers avec un shim. Le shim traduit, ou mappe, le format de vRealize Log Insight en un format différent.

Les notifications système, les alertes créées avec des requêtes de message et les alertes créées avec des requêtes agrégées disposent chacune de leur propre format webhook.

Vous devez être un administrateur vRealize Log Insight pour créer des notifications système.

L'authentification de base HTTP est prise en charge. Incorporer des informations d'identification dans l'url en utilisant le formulaire `{{https://username:password@hostname/path}}`

Format de webhook pour une notification système

Le format d'un webhook vRealize Log Insight dépend du type de requête à partir de laquelle il est créé. Les notifications système, les requêtes de message d'alerte utilisateur et les alertes générées à partir des requêtes utilisateur agrégées disposent chacune d'un format de webhook différent.

Vous devez être un administrateur vRealize Log Insight pour configurer vRealize Log Insight afin qu'il envoie des notifications système.

Lorsque vous envoyez une notification système à un programme tiers, vous devez écrire un shim pour rendre les informations de vRealize Log Insight compréhensibles par les formats du programme tiers.

Format de webhook pour notifications système

L'exemple suivant montre le format de webhook de vRealize Log Insight pour les notifications système.

```
{
  "AlertName": "Admin Alert: Worker node has returned to service (Host = 127.0.0.2)",
  "messages": [
    {
      "text": "This notification was generated from Log Insight node (Host = 127.0.0.2,
Node Identifier = a31cad22-65c2-4131-8e6c-27790892a1f9).
A worker node has returned to service after having been in maintenance mode.
The Log Insight master node reports that worker node has finished maintenance
and exited maintenance mode. The node will resume receiving configuration changes and
serving queries. The node is also now ready to start receiving incoming log messages."
```

```

    "timestamp":1458665320514,"fields":[]
  }
]
}

```

Ajouter une destination de transfert d'événements de vRealize Log Insight

Vous pouvez configurer un serveur vRealize Log Insight pour qu'il transfère les événements entrants vers une cible Syslog ou API Ingestion.

Utilisez le transfert d'événements pour envoyer des événements filtrés ou balisés vers une ou plusieurs destinations distantes comme vRealize Log Insight et/ou Syslog. Cette fonctionnalité peut être utilisée pour prendre en charge les outils de journalisation existants (SIEM, par exemple), ainsi que pour consolider la journalisation sur différents réseaux (DMZ et/ou WAN, par exemple).

Remarque Les redirecteurs d'événements peuvent être autonomes ou en cluster, mais il s'agit d'instances totalement indépendantes de la destination distante. Les instances configurées pour le transfert d'événements stockent aussi les événements localement et peuvent être utilisées pour interroger les données.

Prérequis

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Vérifiez que la destination peut gérer le nombre d'événements qui sont transférés. Si le cluster de destination est plus petit que l'instance de transfert, certains événements pourraient être abandonnés.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Sous Gestion, cliquez sur **Transfert d'événements**.

3 Cliquez sur **Nouvelle destination** et indiquez les informations ci-après.

Option	Description
Nom	Nom unique pour la nouvelle destination.
Hôte	Adresse IP ou nom de domaine complet. Avertissement Une boucle de transfert est une configuration dans laquelle un cluster vRealize Log Insight transfère des événements à lui-même, ou à un autre cluster, qui retransfère ensuite les événements au cluster d'origine. Ce type de boucle peut créer un nombre indéfini de copies de chaque événement transféré. L'interface Web vRealize Log Insight ne vous permet pas de configurer un événement destiné à être envoyé à lui-même. Cependant, vRealize Log Insight ne peut pas empêcher les boucles de transfert indirectes. Par exemple, le cluster A de vRealize Log Insight transfère des événements au cluster B, lequel retransfère ces mêmes événements à A. Lors de la création de destinations de transfert, veuillez donc à ne pas créer de boucles de transfert indirectes.
Protocole	API Ingestion ou syslog. La valeur par défaut est API Ingestion (CFAPI). Lorsque des événements sont transférés à l'aide de l'API Ingestion, la source d'origine de l'événement est conservée dans le champ source. Lorsque des événements sont transférés à l'aide de syslog, la source d'origine de l'événement est perdue et le récepteur peut enregistrer la source du message comme l'adresse IP ou le nom d'hôte du redirecteur vRealize Log Insight. Remarque Le champ source peut contenir différentes valeurs selon le protocole sélectionné dans le redirecteur d'événements : <ul style="list-style-type: none"> a Pour L'API Ingestion, la source est l'adresse IP de l'expéditeur initial (à l'origine de l'événement). b Pour syslog, la source est l'adresse IP de l'instance vRealize Log Insight du redirecteur d'événements. De plus, le texte du message Syslog contient <code>_li_source_path</code>, qui pointe vers l'adresse IP de l'expéditeur initial.
Utiliser SSL	Vous pouvez éventuellement sécuriser la connexion avec SSL pour l'API Ingestion. La racine fiable du serveur distant est validée et le transfert d'événements avec SSL ne fonctionne pas avec les certificats autosignés installés sur les serveurs de destination par défaut. Si elle n'est pas fiable, importez le certificat racine approuvé du serveur dans le keystore du redirecteur. Reportez-vous à Configurer le transfert d'événements de vRealize Log Insight avec SSL .
Balises	Vous pouvez éventuellement ajouter des paires de balises avec des valeurs prédéfinies. Les balises vous permettent d'interroger plus facilement les événements. Vous pouvez ajouter plusieurs balises séparées par des virgules.
Transmettre des balises complémentaires	Vous pouvez indiquer si vous souhaitez transmettre des balises complémentaires pour Syslog. Les balises complémentaires sont les balises ajoutées par le cluster lui-même, telles que « <code>vc_username</code> » ou « <code>vc_vmname</code> ». Elles peuvent être transmises avec les balises provenant directement des sources. Les balises complémentaires sont toujours transférées lorsque l'API Ingestion est utilisée.
Transport	Sélectionnez un protocole de transport pour Syslog. Vous pouvez choisir UDP ou TCP.

- 4 (Facultatif) Pour contrôler les événements à transférer, cliquez sur **+ Ajouter un filtre**.

Sélectionnez des champs et des contraintes pour définir les événements souhaités. Seuls les champs static peuvent être utilisés comme filtres. Si vous ne sélectionnez pas de filtre, tous les événements sont transférés. Vous pouvez consulter les résultats du filtre que vous créez en cliquant sur **Exécuter dans l'analyse interactive**.

Option	Description
correspond	Recherche les chaînes qui correspondent à la chaîne et au caractère générique spécifiés. Par exemple, test* correspond aux chaînes comme test123 ou test-run , mais pas my-test-run . test correspond à test , mais pas test123 .
ne correspond pas	Exclut les chaînes qui correspondent à cette chaîne et au caractère générique spécifiés. Par exemple, test* exclut test123 , mais pas mytest123 .
commence par	Recherche les chaînes qui commencent par la chaîne de caractères spécifiée. Par exemple, test trouve test123 ou test , mais pas my-test123 .
ne commence pas par	Exclut les chaînes qui commencent par la chaîne de caractères spécifiée. Par exemple, test exclut test123 , mais pas my-test123 .

- 5 (Facultatif) Cliquez sur **Afficher les paramètres avancés** pour modifier les informations de transfert suivantes.

Option	Description
Port	Port vers lequel les événements sont envoyés sur la destination distante. Valeur par défaut est définie sur la base du protocole spécifié. Ne pas modifier, sauf si la destination distante écoute sur un port différent.
Cache de disque	Quantité d'espace disque local à réserver pour la mise en mémoire tampon des événements que vous avez configurés pour être transférés. La mise en mémoire tampon est utilisée lorsque la destination distante est indisponible ou dans l'incapacité de traiter les événements qui lui sont envoyés. Si le tampon local est plein et que la destination distante n'est toujours pas disponible, les événements locaux les plus récents sont abandonnés et ne sont pas transférés vers la destination distante, même lorsque celle-ci est en ligne. La valeur par défaut est de 200 Mo.
Nombre de travailleurs	Nombre de connexions sortantes simultanées à utiliser. Définissez un nombre de travailleurs plus élevé pour obtenir une latence du réseau plus élevée vers la destination transférée et un nombre plus élevé d'événements transférés par seconde. La valeur par défaut est 8.

- 6 Pour vérifier votre configuration, cliquez sur **Tester**.

- 7 Cliquez sur **Enregistrer**.

Suivant

- [Configurer le transfert d'événements de vRealize Log Insight avec SSL](#).

- Vous pouvez modifier ou cloner une destination de transfert d'événements. Si vous modifiez la destination pour changer le nom d'un redirecteur d'événements, toutes les statistiques sont réinitialisées.

Configurer le transfert d'événements de vRealize Log Insight avec SSL

Vous pouvez configurer un serveur vRealize Log Insight pour qu'il transfère les événements entrants vers un autre serveur Log Insight via une cible API Ingestion avec SSL.

Prérequis

Le transfert d'événements avec SSL ne fonctionne pas avec le certificat autosigné installé sur les serveurs de destination par défaut. Un certificat SSL personnalisé doit être créé en utilisant les étapes de la section [Générer une demande de signature de certificat](#), puis téléchargé. Reportez-vous à [Installer un certificat SSL personnalisé](#)

Procédure

- 1 Copiez le certificat racine approuvé dans un répertoire temporaire sur l'instance du redirecteur. Par exemple /home.
- 2 SSH vers l'instance du redirecteur et exécutez les commandes suivantes.

```
localhost:~ # cd /usr/java/default/lib/security/
localhost:/usr/java/default/lib/security # ../../bin/keytool
-import -alias loginsight -file /home/cacert.crt -keystore cacerts
```

Le mot de passe par défaut du keystore est **changeit**.

Remarque Les versions de Java peuvent varier dans le temps.

- 3 Redémarrez l'instance de vRealize Log Insight.

Si vous utilisez un environnement de cluster vRealize Log Insight, cette opération doit être effectuée sur tous les nœuds avec le même certificat.

Suivant

Activez la connexion SSL. Reportez-vous à [Appliquer des connexions SSL uniquement](#).

Synchroniser l'heure sur le dispositif virtuel vRealize Log Insight

Vous devez synchroniser l'heure du dispositif virtuel vRealize Log Insight avec celle d'un serveur NTP ou avec celle de l'hôte ESX/ESXi sur lequel le dispositif virtuel est déployé.


La définition précise de l'heure est essentielle au bon fonctionnement des fonctionnalités principales de vRealize Log Insight.

Par défaut, l'heure de vRealize Log Insight se synchronise avec celle d'une liste prédéfinie de serveurs NTP publics. Si les serveurs NTP publics sont bloqués par un pare-feu, vous pouvez utiliser le serveur NTP interne de votre société. Si aucun serveur NTP n'est disponible, vous pouvez synchroniser l'heure avec celle de l'hôte ESX/ESXi sur lequel le dispositif virtuel vRealize Log Insight est déployé.

Prérequis

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Sous Configuration, cliquez sur **Heure**.
- 3 Dans le menu déroulant **Synchroniser l'heure avec**, sélectionnez l'origine de l'heure avec laquelle la synchronisation aura lieu.

Option	Description
serveur NTP	Synchronise l'heure du dispositif virtuel vRealize Log Insight avec celle de l'un des serveurs NTP de la liste.
Hôte ESX/ESXi	Synchronise l'heure du dispositif virtuel vRealize Log Insight avec celle de l'hôte ESX/ESXi sur lequel le dispositif virtuel est déployé.

- 4 (Facultatif) Si vous avez choisi la synchronisation avec le serveur NTP, répertoriez les adresses de serveurs NTP, puis cliquez sur **Tester**.

Remarque Le test de connexion aux serveurs NTP peut prendre jusqu'à 20 secondes par serveur.

- 5 Click **Save**.

Configurer le serveur SMTP pour vRealize Log Insight


Vous pouvez configurer un SMTP pour permettre à vRealize Log Insight d'envoyer des alertes par e-mail.

Les alertes système ont lieu lorsque vRealize Log Insight détecte un événement système important (par exemple, lorsque la capacité de stockage du dispositif virtuel atteint le seuil défini).

Prérequis

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Dans Configuration, cliquez sur **SMTP**.

- 3 Tapez le numéro de port et l'adresse du serveur SMTP.
- 4 Si le serveur SMTP utilise une connexion chiffrée, sélectionnez le protocole de chiffrement.
- 5 Dans la zone de texte **Expéditeur**, tapez l'adresse e-mail à utiliser pour l'envoi des alertes système.
L'adresse de l'**expéditeur** est celle qui s'affiche dans le champ De des e-mails de notification du système. Il n'est pas nécessaire que ce soit une adresse véritable, et elle peut faire référence à l'instance spécifique de vRealize Log Insight. Par exemple, **loginisght@example.com**.
- 6 Tapez un nom d'utilisateur et un mot de passe pour l'authentification auprès du serveur SMTP lors de l'envoi d'alertes système.
- 7 Tapez une adresse e-mail de destination, puis cliquez sur **Envoyer un e-mail de test** pour vérifier la connexion.
- 8 Cliquez sur **Save**.

Installer un certificat SSL personnalisé

Par défaut, vRealize Log Insight installe un certificat SSL auto-signé sur le dispositif virtuel.

Le certificat auto-signé génère des avertissements de sécurité lorsque vous vous connectez à l'interface utilisateur Web de vRealize Log Insight. Si vous ne souhaitez pas utiliser un certificat de sécurité autosigné, vous pouvez installer un certificat SSL personnalisé. Le transfert d'événements via SSL est la seule fonctionnalité nécessitant un certificat SSL personnalisé. Si vous avez une configuration de cluster sur laquelle un équilibrage de charge intégré (ILB, Integrated Load Balancer) est activé, reportez-vous à la section [Activer l'équilibrage de charge intégrée](#) pour connaître les exigences spécifiques d'un certificat SSL personnalisé.

Remarque The vRealize Log Insight Web user interface and the Log Insight Ingestion protocol cfapi use the same certificate for authentication.

Prérequis

- Verify that your custom SSL certificate meets the following requirements.
 - The CommonName contains a wildcard or exact match for the Master node or FQDN of the virtual IP address. Optionally, all other IP addresses and FQDNs are listed as subjectAltName.
 - The certificate file contains both a valid private key and a valid certificate chain.
 - The private key is generated by the RSA or the DSA algorithm.
 - The private key is not encrypted by a pass phrase.
 - If the certificate is signed by a chain of other certificates, all other certificates are included in the certificate file that you plan to import.
 - The private key and all the certificates that are included in the certificate file are PEM-encoded. vRealize Log Insight does not support DER-encoded certificates and private keys.

- The private key and all the certificates that are included in the certificate file are in the PEM format. vRealize Log Insight does not support certificates in the PFX, PKCS12, PKCS7, or other formats.
- Vérifiez que vous concaténez l'intégralité du corps de chaque certificat dans un seul fichier texte dans l'ordre suivant.
 - a La clé privée - *your_domain_name.key*
 - b Le certificat principal- *your_domain_name.crt*
 - c Le certificat intermédiaire - *DigiCertCA.crt*
 - d Le certificat racine - *TrustedRoot.crt*
- Vérifiez que vous incluez les balises de début et de fin de chaque certificat dans le format suivant.

```

-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: your_domain_name.key)
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: your_domain_name.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: DigiCertCA.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Root certificate: TrustedRoot.crt)
-----END CERTIFICATE-----

```

- Verify that you are logged in to the vRealize Log Insight *portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

1 Générer un certificat autosigné

Vous pouvez générer un certificat autosigné pour Windows ou Linux en utilisant l'outil OpenSSL.

2 Générer une demande de signature de certificat

Utilisez l'outil OpenSSL pour Windows pour générer une demande de signature de certificat.

3 Demander la signature d'une autorité de certification

Envoyez votre demande de signature de certificat à l'autorité de certification de votre choix et demandez une signature.

4 Concaténer les fichiers de certificat

Combinez vos fichiers de clé et de certificat sous forme de fichier PEM.

5 Télécharger un certificat signé

Vous pouvez télécharger un certificat SSL signé.

6 Configurer la connexion SSL entre le serveur vRealize Log Insight et Log Insight Agents

La fonction SSL vous permet de fournir des connexions SSL seulement entre Log Insight Agents et le serveur vRealize Log Insight par l'intermédiaire du flux sécurisé de l'API Ingestion. Vous pouvez également configurer divers paramètres SSL de Log Insight Agents.

Générer un certificat autosigné

Vous pouvez générer un certificat autosigné pour Windows ou Linux en utilisant l'outil OpenSSL.

Prérequis

- Téléchargez le programme d'installation d'OpenSSL approprié à l'adresse <https://www.openssl.org/community/binaries.html> et exécutez-le pour installer cet outil sur Windows.
- Modifiez le fichier `openssl.cfg` pour ajouter d'autres paramètres requis. Assurez-vous que le paramètre `req_extensions` est défini dans la section `[req]`.

```
[req]
.
.
req_extensions=v3_req #
```

- Ajoutez une entrée Autre nom du sujet pour le nom d'hôte ou l'adresse IP de votre serveur, par exemple `server-01.loginsight.domain`. Vous ne pouvez pas spécifier de modèle pour le nom d'hôte.

```
[v3_req]
.
.
subjectAltName=DNS:server-01.loginsight.domain
#subjectAltName=IP:10.27.74.215
```

Procédure

- 1 Créez un dossier dans lequel enregistrer vos fichiers de certificat, par exemple `C:\Certs\LogInsight`.
- 2 Ouvrez une invite de commande et saisissez la commande suivante.

```
C:\Certs\LogInsight>openssl req -x509 -nodes -newkey 2048 -keyout server.key -out server.crt -days 3650
```

OpenSSL vous invite à fournir les propriétés du certificat, dont le pays, l'organisation, etc.

- 3 Entrez l'adresse IP exacte ou le nom d'hôte exact de votre serveur vRealize Log Insight, ou bien l'adresse du cluster vRealize Log Insight si l'équilibrage de charge est activé.

La propriété est la seule pour laquelle il est obligatoire de spécifier une valeur.

Deux fichiers sont créés, `server.key` et `server.crt`.

- `server.key` est une nouvelle clé privée au format PEM.

- `server.crt` est un nouveau certificat codé au format PEM signé par `server.key`.

Suivant

- Concaténer les fichiers de certificat. Reportez-vous à [Concaténer les fichiers de certificat](#).
- Télécharger le certificat signé. Reportez-vous à [Télécharger un certificat signé](#).

Générer une demande de signature de certificat

Utilisez l'outil OpenSSL pour Windows pour générer une demande de signature de certificat.

Prérequis

- Téléchargez le programme d'installation d'OpenSSL approprié à l'adresse <http://www.openssl.org/related/binaries.html> et exécutez-le pour installer cet outil sur Windows.
- Modifiez le fichier `openssl.cfg` pour ajouter d'autres paramètres requis. Assurez-vous que le paramètre `req_extensions` est défini dans la section `[req]`.

```
[req]
.
.
req_extensions=v3_req #
```

- Ajoutez une entrée Autre nom du sujet pour le nom d'hôte ou l'adresse IP de votre serveur, par exemple `server-01.loginsight.domain`. Vous ne pouvez pas spécifier de modèle pour le nom d'hôte.

```
[v3_req]
.
.
subjectAltName=DNS:server-01.loginsight.domain
#subjectAltName=IP:10.27.74.215
```

Procédure

- 1 Créez un dossier dans lequel enregistrer vos fichiers de certificat, par exemple `C:\Certs\LogInsight`.
- 2 Ouvrez une invite de commande et générez votre clé privée en exécutant la commande suivante.

```
C:\Certs\LogInsight>openssl genrsa -out server.key 2048
```

- 3 Créez une demande de signature de certificat en exécutant la commande suivante.

```
C:\Certs\LogInsight>openssl req -new -key server.key -out server.csr
```

Remarque Cette commande s'exécute de manière interactive et vous pose un certain nombre de questions. Votre autorité de certification vérifiera la correspondance de vos réponses avec les informations incluses dans les documents légaux relatifs à l'inscription de votre société.

- 4 Suivez les instructions à l'écran et entrez les informations qui seront incorporées à votre demande de certificat.

Important Dans le champ Nom commun, entrez le nom d'hôte ou l'adresse IP de votre serveur, par exemple `mail.your.domain`. Si vous souhaitez inclure tous les sous-domaines, entrez `*your.domain`.

Votre fichier de demande de signature de certificat `server.csr` est généré et enregistré.

Demander la signature d'une autorité de certification

Envoyez votre demande de signature de certificat à l'autorité de certification de votre choix et demandez une signature.

Procédure

- ◆ Envoyez votre fichier `server.csr` à une autorité de certificat.

Remarque Demandez à l'autorité de certificat que le fichier soit codé au format PEM.

L'autorité de certificat traite votre demande et vous renvoie un fichier `server.crt` codé au format PEM.

Concaténer les fichiers de certificat

Combinez vos fichiers de clé et de certificat sous forme de fichier PEM.

Procédure

- 1 Créez un nouveau fichier `server.pem` et ouvrez-le dans un éditeur de texte.
- 2 Copiez le contenu de votre fichier `server.key` et collez-le dans le fichier `server.pem` selon le format suivant.

```
-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: server.key)
-----END RSA PRIVATE KEY-----
```

- 3 Copiez le contenu de votre fichier `server.crt` et collez-le dans le fichier `server.pem` selon le format suivant.

```
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: server.crt)
-----END CERTIFICATE-----
```

- 4 Si les Autorités de certification vous ont fourni un certificat intermédiaire ou lié, ajoutez-le à la fin du fichier de certificat public selon le format suivant.


```
-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: server.key)
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: server.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: DigiCertCA.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Root certificate: TrustedRoot.crt)
-----END CERTIFICATE-----
```

- 5 Enregistrez votre fichier `server.pem`.

Télécharger un certificat signé

Vous pouvez télécharger un certificat SSL signé.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Sous Configuration, cliquez sur **Certificat SSL**.
- 3 Accédez à votre certificat SSL personnalisé et cliquez sur **Ouvrir**.
- 4 Click **Save**.
- 5 Redémarrez vRealize Log Insight.

Suivant

After vRealize Log Insight restarts, verify that syslog feeds from ESXi continue to arrive in vRealize Log Insight. For troubleshooting, see [ESXi Logs Stop Arriving in Log Insight](#).

Configurer la connexion SSL entre le serveur vRealize Log Insight et Log Insight Agents

La fonction SSL vous permet de fournir des connexions SSL seulement entre Log Insight Agents et le serveur vRealize Log Insight par l'intermédiaire du flux sécurisé de l'API Ingestion. Vous pouvez également configurer divers paramètres SSL de Log Insight Agents.

Les agents vRealize Log Insight communiquent sur TLSv.1.2. SSLv.3/TLSv.1.0 est désactivé pour répondre aux exigences de sécurité.

Principales fonctions SSL

Comprendre les principales fonctions SSL peut vous aider à configurer correctement Log Insight Agents.

L'agent vRealize Log Insight stocke les certificats et les utilise pour vérifier l'identité du serveur durant toutes les connexions, sauf la première connexion à un serveur particulier. Si l'identité du serveur ne peut pas être confirmée, l'agent vRealize Log Insight rejette la connexion au serveur et écrit un message d'erreur correspondant dans le journal. Les certificats reçus par l'agent sont stockés dans le dossier cert.

- Pour Windows, accédez à `C:\ProgramData\VMware\Log Insight Agent\cert`.
- Pour Linux, accédez à `/var/lib/loginsight-agent/cert`.

Lorsque l'agent vRealize Log Insight établit une connexion sécurisée avec le serveur vRealize Log Insight, il vérifie la validité du certificat reçu du serveur vRealize Log Insight. L'agent vRealize Log Insight utilise des certificats racines approuvés par le système.

- Log Insight Linux Agent charge les certificats approuvés à partir de `/etc/pki/tls/certs/ca-bundle.crt` ou de `/etc/ssl/certs/ca-certificates.crt`.
- Log Insight Windows Agent utilise les certificats racines du système.

Si l'agent vRealize Log Insight dispose d'un certificat auto-signé stocké localement et reçoit un certificat auto-signé valide différent avec la même clé publique, il accepte le nouveau certificat. Cela peut se produire lorsqu'un certificat auto-signé est régénéré au moyen de la même clé privée, mais avec des informations différentes telles qu'une nouvelle date d'expiration. Sinon, la connexion est rejetée.

Si l'agent vRealize Log Insight dispose d'un certificat auto-signé stocké localement et reçoit un certificat valide signé par une autorité de certification, l'agent vRealize Log Insight remplace le nouveau certificat accepté en mode silencieux.

Si l'agent vRealize Log Insight reçoit un certificat auto-signé après avoir eu un certificat signé par une autorité de certification, il le rejette. L'agent vRealize Log Insight accepte le certificat auto-signé reçu du serveur vRealize Log Insight uniquement lorsqu'il se connecte à ce serveur pour la première fois.

Si l'agent vRealize Log Insight dispose d'un certificat signé par une autorité de certification stocké localement et reçoit un certificat valide signé par une autre autorité de certification approuvée, il le rejette. Vous pouvez modifier les options de configuration de l'agent vRealize Log Insight pour qu'il accepte le nouveau certificat. Reportez-vous à [Configurer les paramètres SSL de l'agent vRealize Log Insight](#).

Les agents vRealize Log Insight communiquent sur TLSv.1.2. SSLv.3/TLSv.1.0 est désactivé pour répondre aux exigences de sécurité.

Appliquer des connexions SSL uniquement


Vous pouvez utiliser l'interface utilisateur Web de vRealize Log Insight pour configurer vRealize Log Insight Agents et l'API Ingestion pour autoriser uniquement les connexions SSL au serveur.

Normalement, l'API vRealize Log Insight est accessible via HTTP sur le port 9000 et via HTTPS sur le port 9543. Les deux ports peuvent être utilisés par l'agent vRealize Log Insight ou par des clients d'API personnalisés. Toutes les demandes authentifiées requièrent SSL, mais les demandes non authentifiées, notamment le trafic d'ingestion de l'agent vRealize Log Insight, peuvent être exécutées avec l'un ou l'autre. Vous pouvez forcer toutes les demandes d'API à utiliser des connexions SSL. L'option ne limite pas le trafic du port 514 Syslog et n'affecte pas l'interface utilisateur de vRealize Log Insight, pour laquelle les demandes du port 80 HTTP continuent à être redirigées vers le port 443 HTTPS.

Prérequis

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Dans Configuration, cliquez sur **SSL**.
- 3 Sous l'API pour serveur SSL, sélectionnez **Exiger une connexion SSL**.
- 4 Click **Save**.

L'API vRealize Log Insight autorise uniquement les connexions SSL au serveur. Les connexions non-SSL sont refusées.

Configurer les paramètres SSL de l'agent vRealize Log Insight

Vous pouvez modifier les fichiers de configuration de l'agent vRealize Log Insight afin de modifier la configuration SSL, d'ajouter un chemin d'accès aux certificats racines approuvés et de définir quels certificats sont acceptés par l'agent.

Cette procédure s'applique aux agents vRealize Log Insight pour Windows et Linux.

Prérequis

Pour l'agent vRealize Log Insight Linux :

- Connectez-vous en tant que **root** ou utilisez `sudo` pour exécuter des commandes de console.
- Connectez-vous à la machine Linux sur laquelle vous avez installé l'agent vRealize Log Insight Linux, ouvrez une console et exécutez `pgrep liagent` pour vérifier que l'agent vRealize Log Insight Linux est installé et fonctionne.

Pour l'agent vRealize Log Insight Windows :

- Log in to the Windows machine on which you installed the vRealize Log Insight Windows agent and start the Services manager to verify that the vRealize Log Insight agent service is installed.

Procédure

- 1 Accédez au dossier contenant le fichier `liagent.ini`.

Système d'exploitation	Chemin
Linux	<code>/var/lib/loginsight-agent/</code>
Windows	<code>%ProgramData%\VMware\Log Insight Agent</code>

- 2 Open the `liagent.ini` file in any text editor.
- 3 Ajoutez les clés suivantes à la section `[server]` du fichier `liagent.ini`.

Clé	Description
<code>ssl_ca_path</code>	<p>Remplace le chemin de stockage par défaut des certificats signés par une autorité de certification racine, qui sont utilisés pour vérifier les certificats d'homologue de connexion.</p> <p>Linux : si aucune valeur n'est spécifiée, l'agent tente de charger des certificats approuvés à partir du fichier <code>/etc/pki/tls/certs/ca-bundle.crt</code> ou <code>/etc/ssl/certs/ca-certificates.crt</code>.</p> <p>Windows : si aucune valeur n'est spécifiée, l'agent vRealize Log Insight Windows charge des certificats à partir du magasin de certificats racine de Windows.</p> <p>Lorsqu'un chemin d'accès pour <code>ssl_ca_path</code> est spécifié, il remplace les valeurs par défaut des agents Linux et Windows. Vous pouvez spécifier comme valeur un fichier dans lequel plusieurs certificats au format PEM sont concaténés ou un répertoire contenant des certificats au format PEM et portant des noms tels que <code>hash.0</code> (voir l'option <code>-hash</code> de l'utilitaire <code>x509</code>).</p>
<code>ssl_accept_any</code>	<p>Indique si des certificats sont acceptés par l'agent vRealize Log Insight. Les valeurs possibles sont <code>yes</code>, <code>1</code>, <code>no</code> ou <code>0</code>. Lorsque la valeur est définie sur <code>yes</code> ou <code>1</code>, l'agent accepte n'importe quel certificat du serveur et établit une connexion sécurisée pour l'envoi des données. La valeur par défaut est <code>no</code>.</p>

Clé	Description
ssl_accept_any_trusted	Les valeurs possibles sont yes, 1, no ou 0. Si l'agent vRealize Log Insight dispose d'un certificat signé approuvé par une autorité de certification stocké localement et reçoit un certificat valide différent signé par une autre autorité de certification approuvée, il vérifie l'option de configuration. Si la valeur est définie sur yes ou 1, l'agent accepte le nouveau certificat valide. Si la valeur est définie sur no ou sur 0, il rejette le certificat et met fin à la connexion. La valeur par défaut est no.
ssl_cn	Common Name du certificat auto-signé. La valeur par défaut est VMware vCenter Log Insight. Vous pouvez définir un Common Name personnalisé devant être vérifié par rapport au champ Common Name du certificat. L'agent vRealize Log Insight vérifie le champ Common Name du certificat reçu par rapport au nom d'hôte spécifié pour la clé hostname dans la section [server]. En l'absence de correspondance, l'agent vérifie le champ Common Name par rapport à la clé ssl_cn dans le fichier liagent.ini. Si les valeurs correspondent, l'agent vRealize Log Insight accepte le certificat.

Remarque Ces clés sont ignorées si SSL est désactivé.

- 4 Save and close the liagent.ini file.

Exemple : Configuration

Vous trouverez ci-dessous un exemple de la configuration SSL.

```
proto=cfapi
port=9543
ssl=yes
ssl_ca_path=/etc/pki/tls/certs/ca-bundle.crt
ssl_accept_any=no
ssl_accept_any_trusted=yes
ssl_cn=LOGINSIGHT
```

Modifier le délai d'expiration par défaut des sessions Web de vRealize Log Insight


Par défaut, afin de maintenir votre environnement en sécurité, les sessions Web de vRealize Log Insight expirent au bout de 30 minutes. Vous pouvez modifier ce paramètre et définir un délai d'expiration plus court ou plus long.

Vous pouvez modifier le délai d'expiration en utilisant l'interface utilisateur Web.

Prérequis

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Configuration, click **General**.
- 3 Dans le volet Session de navigateur, spécifiez une valeur du délai d'expiration en minutes.
La valeur `-1` désactive le délai d'expiration des sessions.
- 4 Click **Save**.

Archives

Activer ou désactiver l'archivage des données dans vRealize Log Insight

L'archivage des données vous permet de conserver les anciens événements de journaux, qui risqueraient d'être supprimés du dispositif virtuel vRealize Log Insight en raison des contraintes de stockage. vRealize Log Insight peut stocker des données archivées sur des montages NFS.

vRealize Log Insight collecte et enregistre les journaux sur le disque dans une série de compartiments d'1 Go. Un compartiment est constitué de fichiers journaux compressés et d'un index. Un compartiment contient tout ce qui est nécessaire pour effectuer des requêtes pendant un intervalle de temps spécifique. Lorsque la taille du compartiment dépasse 1 Go, vRealize Log Insight cesse d'écrire, ferme tous les fichiers du compartiment et scelle celui-ci.

Lors de l'archivage des données, vRealize Log Insight copie les fichiers journaux compressés bruts à partir du compartiment vers un montage NFS lorsque le compartiment est scellé. Les compartiments qui ont été scellés alors que l'archivage des données n'était pas activé ne sont pas archivés rétroactivement.

Le chemin créé lors d'un export d'archive est sous la forme


year/month/day/hour/bucketuuid/data.blob et l'heure utilisée est celle à laquelle le compartiment a été initialement créé en temps UTC.

Remarque vRealize Log Insight ne gère pas le montage NFS utilisé pour l'archivage. Si les notifications système sont activées, vRealize Log Insight envoie un e-mail lorsque le montage NFS n'a presque plus d'espace ou est indisponible. Si le montage NFS ne dispose pas de suffisamment d'espace disponible ou s'il n'est pas disponible pendant une durée supérieure à la période de rétention du dispositif virtuel, vRealize Log Insight cesse d'ingérer de nouvelles données. L'ingestion de données reprend lorsque le montage NFS dispose de suffisamment d'espace libre, qu'il est de nouveau disponible, ou que l'archivage est désactivé.

Prérequis

- Vérifiez que vous avez accès à une partition NFS qui remplit les critères suivants.
 - La partition NFS doit permettre aux comptes invités de réaliser des opérations de lecture et d'écriture.
 - Le montage ne doit nécessiter aucune authentification.
 - Le serveur NFS doit prendre en charge NFS v3.
 - Si vous utilisez un serveur Windows NFS, autorisez un accès utilisateurs UNIX non mappé (par UID/GID).
- Verify that you are logged in to the vRealize Log Insight *portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Dans Configuration, cliquez sur **Archivage**.
- 3 Sélectionnez **Activer l'archivage des données** et entrez le chemin d'accès à une partition NFS dans laquelle les journaux seront archivés sous la forme `nfs://servername<:port-number>/exportname`.

Le numéro de port par défaut est 2049.
- 4 Cliquez sur **Tester** pour vérifier la connexion.
- 5 Cliquez **Save**.

Remarque L'archivage des données vous permet de conserver les anciens journaux qui sont supprimés du dispositif virtuel vRealize Log Insight en raison des contraintes de stockage. Vous ne pouvez plus rechercher les événements de journaux ayant été supprimés du dispositif virtuel vRealize Log Insight et archivés. Si vous souhaitez rechercher des journaux archivés, vous devez les importer dans une instance de vRealize Log Insight. Pour plus d'informations sur l'importation de fichiers journaux archivés, consultez la section [Importer une archive vRealize Log Insight dans vRealize Log Insight](#).

Suivant

After vRealize Log Insight restarts, verify that syslog feeds from ESXi continue to arrive in vRealize Log Insight. For troubleshooting, see [ESXi Logs Stop Arriving in Log Insight](#).

Format des fichiers d'archives de vRealize Log Insight

vRealize Log Insight archive les données dans un format spécifique.

vRealize Log Insight stocke les fichiers d'archives sur un serveur NFS et les organise en répertoires hiérarchiques en fonction de l'heure d'archivage. Par exemple,

`/backup/2014/08/07/16/bd234b2d-df98-44ae-991a-e0562f10a49/data.blob`

où `/backup` est l'emplacement NFS, `2014/08/07/16` est l'heure d'archivage, `bd234b2d-df98-44ae-991a-e0562f10a49` est l'ID de compartiment et `data.blob` correspond aux données archivées du compartiment.

Les données d'archive `data.blob` sont un fichier compressé qui utilise un codage interne de vRealize Log Insight. Il renferme le contenu d'origine de tous les messages stockés dans le compartiment, avec les champs statiques tels qu'horodatage, nom d'hôte, source et nom d'application.

Vous pouvez importer des données archivées dans vRealize Log Insight, exporter des données d'archive dans un fichier texte brut et extraire du contenu de message provenant de données d'archive. Voir [Exporter une archive Log Insight vers un fichier texte brut ou au format JSON](#) et [Importer une archive vRealize Log Insight dans vRealize Log Insight](#).

Importer une archive vRealize Log Insight dans vRealize Log Insight

L'archivage des données vous permet de conserver les anciens journaux qui risqueraient d'être supprimés du dispositif virtuel vRealize Log Insight en raison des contraintes de stockage. Reportez-vous à [Activer ou désactiver l'archivage des données dans vRealize Log Insight](#). Vous pouvez utiliser la ligne de commande pour importer des journaux qui ont été archivé dans vRealize Log Insight.

Remarque Bien que vRealize Log Insight puisse gérer à la fois des données historiques et des données en temps réel, il est recommandé de déployer une instance séparée de vRealize Log Insight pour le traitement des fichiers journaux importés.

Prérequis

- Verify that you have the root user credentials to log in to the vRealize Log Insight virtual appliance.
- Vérifiez que vous avez accès au serveur NFS sur lequel les journaux vRealize Log Insight sont archivés.
- Vérifiez que l'espace disque disponible sur le dispositif virtuel vRealize Log Insight est suffisant pour prendre en charge les fichiers journaux importés.

L'espace libre minimal dans la partition `/storage/core` sur le dispositif virtuel doit correspondre à environ 10 fois la taille du journal archivé à importer.

Procédure

- 1 Établissez une connexion SSH au vApp vRealize Log Insight, puis connectez-vous en tant qu'utilisateur `racine`.
- 2 Montez le dossier partagé sur le serveur NFS où se trouvent les données archivées.

- 3 Pour importer un répertoire de journaux vRealize Log Insight archivés, exécutez la commande suivante.

```
/usr/lib/loginsight/application/bin/loginsight repository import Path-To-Archived-Log-Data-Folder.
```

Remarque Selon la taille du dossier importé, l'importation de données archivées peut prendre beaucoup de temps.

- 4 Fermez la connexion SSH.

Suivant

Vous pouvez rechercher, filtrer et analyser les événements des journaux importés.

Exporter une archive Log Insight vers un fichier texte brut ou au format JSON

Vous pouvez utiliser la ligne de commande pour exporter une archive de vRealize Log Insight vers un fichier texte brut standard ou au format JSON.

Remarque Il s'agit d'une procédure avancée. Les formats de sortie et de syntaxe de commande peuvent être modifiés dans les versions ultérieures de vRealize Log Insight sans compatibilité descendante.

Prérequis

- Verify that you have the root user credentials to log in to the vRealize Log Insight virtual appliance.
- Vérifiez que le dispositif virtuel de vRealize Log Insight dispose de l'espace disque nécessaire pour enregistrer les fichiers exportés.

Procédure

- 1 Établissez une connexion SSH au vApp vRealize Log Insight, puis connectez-vous en tant qu'utilisateur racine.
- 2 Créez un répertoire d'archivage sur le vApp de vRealize Log Insight.

```
mkdir /archive
```

- 3 Montez le dossier partagé sur le serveur NFS où les données archivées résident en exécutant la commande suivante.

```
mount -t nfs archive-fileshare:archive directory path /archive
```

- 4 Vérifiez l'espace de stockage disponible sur le vApp de vRealize Log Insight.

```
df -h
```

- 5 Exportez une archive de vRealize Log Insight vers un fichier texte brut.

```
/usr/lib/loginsight/application/sbin/repo-exporter -d archive-file-directory output-file
```

Par exemple,

```
/usr/lib/loginsight/application/sbin/repo-exporter -d /archive/2014/08/07/16/bd234b2d-  
df98-44ae-991a-e0562f10a49 /tmp/output.txt
```

- 6 Exportez un contenu de message d'archivage de vRealize Log Insight au format JSON.

```
/usr/lib/loginsight/application/sbin/repo-exporter -F -d archive-file-directory output-file.
```

Par exemple,

```
/usr/lib/loginsight/application/sbin/repo-exporter -F -d /archive/2014/08/07/16/bd234b2d-  
df98-44ae-991a-e0562f10a49 /tmp/output.json
```

- 7 Fermez la connexion SSH.

Redémarrer le service vRealize Log Insight


Vous pouvez utiliser la page d'administration de l'interface utilisateur Web pour redémarrer vRealize Log Insight.

Avertissement Le redémarrage de vRealize Log Insight entraîne la fermeture de toutes les sessions utilisateurs actives. Les utilisateurs de l'instance de vRealize Log Insight seront forcés à se connecter de nouveau.

Prérequis

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Cluster**.
- 3 Sélectionnez un nœud de cluster.
- 4 Cliquez sur **Redémarrer l'hôte principal**, puis sur **Redémarrer**.

Suivant

After vRealize Log Insight restarts, verify that syslog feeds from ESXi continue to arrive in vRealize Log Insight. For troubleshooting, see [ESXi Logs Stop Arriving in Log Insight](#).

Mettre le dispositif virtuel vRealize Log Insight hors tension

Afin d'éviter la perte de données lorsqu'un nœud maître ou travailleur vRealize Log Insight est mis hors tension, vous devez suivre les étapes de mise hors tension dans un ordre strict.

Vous devez mettre le dispositif virtuel vRealize Log Insight hors tension avant d'apporter des modifications à son matériel virtuel.

Mettez le dispositif virtuel vRealize Log Insight hors tension à l'aide de l'option de menu **Alimentation > Arrêter l'invité** dans vSphere Client, avec la console du dispositif virtuel ou bien en établissant une connexion SSH avec le dispositif virtuel vRealize Log Insight et en exécutant une commande.

Prérequis

- If you plan to connect to the vRealize Log Insight virtual appliance by using SSH, verify that TCP port 22 is open.
- Verify that you have the root user credentials to log in to the vRealize Log Insight virtual appliance.

Procédure

- 1 Établissez une connexion SSH au vApp vRealize Log Insight, puis connectez-vous en tant qu'utilisateur racine.
- 2 Pour mettre le dispositif virtuel vRealize Log Insight hors tension, exécutez `shutdown -h now`.

Suivant

Vous pouvez apporter des modifications au matériel virtuel du dispositif virtuel vRealize Log Insight en toute sécurité.

Télécharger un bundle de support vRealize Log Insight

Si vRealize Log Insight ne fonctionne pas comme prévu en raison d'un problème, vous pouvez envoyer une copie des fichiers de configuration et du journal au support VMware sous la forme d'un bundle de support.

Il n'est nécessaire de télécharger un bundle de support pour cluster que si les services de support de VMware vous le demandent. Vous pouvez créer le bundle de façon statique, c'est-à-dire qu'il utilise l'espace disque sur le nœud, ou par diffusion, c'est-à-dire qu'il n'utilise pas d'espace disque sur le nœud et qu'il stocke le bundle sur votre machine initiale par défaut.

Prérequis

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

1 Click the configuration drop-down menu icon  and select **Administration**.

2 Sous Gestion, cliquez sur **Cluster**.

3 Sous l'en-tête Support, cliquez sur **Télécharger un bundle de support**.

Le système vRealize Log Insight collecte les informations de diagnostic et envoie les données à votre navigateur dans un tarball compressé.

4 Choisissez la méthode pour créer le bundle.

- Sélectionnez **Bundle de support statique** pour créer un bundle localement. La création du bundle consomme de l'espace disque sur le nœud.
- Sélectionnez **Bundle de support de diffusion** pour commencer la diffusion du bundle de support immédiatement. Cette méthode n'utilise pas d'espace disque sur le nœud.

5 Cliquez sur **Continuer**.

6 Dans la boîte de dialogue Téléchargement du fichier, cliquez sur **Enregistrer**.

7 Sélectionnez l'emplacement d'enregistrement de l'archive tarball, puis cliquez sur **Enregistrer**.

Suivant

Vous pouvez rechercher les messages d'erreur dans le contenu des fichiers journaux. Lorsque vous résolvez un problème ou que vous y mettez fin, supprimez le bundle de support obsolète pour économiser de l'espace disque.

Rejoindre ou quitter le programme d'amélioration du produit VMware

Vous pouvez rejoindre ou quitter le programme d'amélioration du produit VMware après le déploiement de vRealize Log Insight

Vous choisissez de participer ou non au programme d'amélioration du produit lorsque vous installez vRealize Log Insight. Après l'installation, vous pouvez rejoindre ou quitter le programme en procédant comme suit.

Prérequis

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

1 Click the configuration drop-down menu icon  and select **Administration**.

2 Under Configuration, click **General**.

- 3 Dans le volet Programme d'amélioration du produit, cochez ou décochez la case **Participer au programme d'amélioration du produit VMware**.

Lorsque cette option est sélectionnée, elle active le Programme et envoie des données à <https://vmware.com>.

- 4 Cliquez **Save**.

Configuration des clusters vRealize Log Insight

5

Vous pouvez ajouter, supprimer et mettre à niveau les nœuds d'un cluster vRealize Log Insight.

Remarque La mise en clusters de réseau étendu n'est pas prise en charge par vRealize Log Insight. Les versions actuelles de vRealize Log Insight ne prennent pas en charge la mise en clusters de réseau étendu (également nommée geoclustering, mise en clusters haute disponibilité ou mise en clusters à distance). Tous les nœuds du cluster doivent être déployés dans le même réseau local de couche 2. En outre, les ports décrits dans [Ports et interfaces externes](#) doivent être ouverts entre les nœuds pour garantir une bonne communication.

Ce chapitre aborde les rubriques suivantes :

- [Ajouter un nœud travailleur à un cluster vRealize Log Insight](#)
- [Supprimer un nœud travailleur d'un cluster vRealize Log Insight](#)
- [Utilisation de l'équilibrage de charge intégrée](#)
- [Interroger les résultats des vérifications du cluster en production](#)

Ajouter un nœud travailleur à un cluster vRealize Log Insight

Déployez une nouvelle instance du dispositif virtuel Log Insight et ajoutez-la à un nœud maître Log Insight existant.

Procédure

1 [Déployer le dispositif virtuel vRealize Log Insight](#)

Téléchargez le dispositif virtuel vRealize Log Insight. VMware distribue le dispositif virtuel vRealize Log Insight sous forme de fichier .ova. Vous pouvez déployer le dispositif virtuel vRealize Log Insight à l'aide de vSphere Client.

2 [Rejoindre un déploiement existant](#)

Une fois que vous avez déployé et configuré un nœud autonome vRealize Log Insight, vous pouvez déployer une nouvelle instance de vRealize Log Insight et l'ajouter au nœud existant afin de créer un cluster vRealize Log Insight.

Déployer le dispositif virtuel vRealize Log Insight

Téléchargez le dispositif virtuel vRealize Log Insight. VMware distribue le dispositif virtuel vRealize Log Insight sous forme de fichier .ova. Vous pouvez déployer le dispositif virtuel vRealize Log Insight à l'aide de vSphere Client.

Prérequis

- Vérifiez que vous disposez d'une copie du fichier .ova du dispositif virtuel vRealize Log Insight.
- Vérifiez que vous disposez des autorisations requises pour déployer les modèles OVF dans l'inventaire.
- Vérifiez que votre environnement dispose des ressources nécessaires à la mise en place de la configuration minimale requise pour le dispositif virtuel vRealize Log Insight. Reportez-vous à [Configuration minimale requise](#).
- Assurez-vous de prendre connaissance des recommandations en matière de dimensionnement pour le dispositif virtuel. Reportez-vous à [Dimensionnement du dispositif virtuel Log Insight](#).

Procédure

- 1 Dans vSphere Client, sélectionnez **Fichier > Déployer le modèle OVF**.
- 2 Suivez les invites de l'assistant **Déployer le modèle OVF**.
- 3 Sur la page Sélectionner une configuration, sélectionnez la taille du dispositif virtuel vRealize Log Insight à partir de la taille de l'environnement dans lequel vous souhaitez collecter les journaux.

L'option **Petite** correspond à la configuration minimale requise pour les environnements de production.

vRealize Log Insight fournit des tailles de VM prédéfinies que vous pouvez choisir pour répondre aux exigences d'ingestion de votre environnement. Il s'agit de combinaisons de tailles certifiées de ressources de calcul et de disque, mais vous pouvez ajouter des ressources supplémentaires par la suite. Une petite configuration consomme le moins de ressources possible tout en restant prise en charge. Une très petite configuration n'est appropriée que pour les démos.

Option	Taux d'ingestion des journaux	CPU virtuels	Mémoire	IOPS	Connexions Syslog (connexions TCP actives)	Événements par seconde
Très petite	6 Go/jour	2	4 Go	75	20	400
Petite	30 Go/jour	4	8 Go	500	100	2000

Option	Taux d'ingestion des journaux	CPU virtuels	Mémoire	IOPS	Connexions Syslog (connexions TCP actives)	Événements par seconde
Moyenne	75 Go/jour	8	16 Go	1 000	250	5000
Grande	225 Go/jour	16	32 Go	1 500	750	15 000

Remarque Vous pouvez utiliser un agrégateur syslog pour augmenter le nombre de connexions syslog qui envoient des événements à vRealize Log Insight. Cependant, le nombre maximal d'événements par seconde est fixe et ne dépend pas de l'utilisation d'un agrégateur syslog. Une instance de vRealize Log Insight ne peut pas être utilisée comme agrégateur syslog.

Remarque Si vous choisissez **Grande**, vous devez effectuer la mise à niveau du matériel virtuel sur la machine virtuelle vRealize Log Insight après le déploiement.

4 Sur la page Sélectionner un stockage, sélectionnez un format de disque.

- **Provisionnement statique mis à zéro en différé** crée un disque virtuel dans un format épais par défaut. L'espace nécessaire pour le disque virtuel est alloué lorsque le disque virtuel est créé. Les données restant sur le périphérique physique ne sont pas effacées lors de la création. Elles sont mises à zéro ultérieurement à la demande, lors de la première écriture effectuée par la machine virtuelle.
- **Provisionnement statique immédiatement mis à zéro** crée un type de disque virtuel statique qui prend en charge des fonctions de mise en cluster telles que la tolérance aux pannes. L'espace nécessaire au disque virtuel est alloué lors de la création. Contrairement au format plat, les données qui restent sur le périphérique physique sont mises à zéro lors de la création du disque virtuel. La création de disques dans ce format peut être plus longue que pour d'autres types de disques.

Important Autant que possible, déployez le dispositif virtuel vRealize Log Insight sur des disques à provisionnement statique immédiatement mis à zéro pour obtenir de meilleures performances et un fonctionnement optimal.

- **Provisionnement dynamique** crée un disque dans le format léger. Le disque se développe à mesure que les données qui y sont enregistrées augmentent. Si votre périphérique de stockage ne prend pas en charge les disques à provisionnement statique ou si vous souhaitez conserver l'espace disque inutilisé sur le dispositif virtuel vRealize Log Insight, déployez ce dernier à l'aide de disques à provisionnement dynamique.

Remarque La réduction de disques sur le dispositif virtuel vRealize Log Insight n'est pas prise en charge et peut entraîner la corruption ou la perte des données.

- 5 (Facultatif) Sur la page Configurer des réseaux, définissez les paramètres de mise en réseau du dispositif virtuel vRealize Log Insight.

Si vous n'indiquez pas de paramètres réseau (comme l'adresse IP, les serveurs DNS et les informations de passerelle), vRealize Log Insight les définit par le biais du protocole DHCP.

Avertissement N'indiquez pas plus de deux serveurs de noms de domaine. Si vous en indiquez plus de deux, le dispositif virtuel vRealize Log Insight ignore tous les serveurs de noms de domaine configurés.

Utilisez une liste séparée par des virgules pour spécifier les serveurs de nom de domaine.

- 6 (Facultatif) Sur la page Personnaliser le modèle, définissez des propriétés réseau si vous n'utilisez pas DHCP.
- 7 (Facultatif) Sur la page Personnaliser le modèle, sélectionnez **Autres propriétés** et définissez le mot de passe racine du dispositif virtuel vRealize Log Insight.

Le mot de passe racine est requis pour SSH. Vous pouvez également définir ce mot de passe via VMware Remote Console.

- 8 Suivez les invites pour finaliser le déploiement.

Pour plus d'informations sur le déploiement des dispositifs virtuels, reportez-vous au *Guide de l'utilisateur pour le déploiement des vApps et des dispositifs virtuels*.

Après la mise sous tension du dispositif virtuel, le processus d'initialisation commence. Ce processus peut prendre plusieurs minutes ; lorsque celui-ci est terminé, le dispositif virtuel redémarre.

- 9 Allez à l'onglet **Console** et vérifiez l'adresse IP du dispositif virtuel vRealize Log Insight.

Préfixe d'adresse IP	Description
https://	DHCP est correctement configuré sur le dispositif virtuel.
http://	La configuration de DHCP sur le dispositif virtuel a échoué. <ul style="list-style-type: none"> a Mettez le dispositif virtuel vRealize Log Insight hors tension. b Cliquez avec le bouton droit sur le dispositif virtuel et sélectionnez Modifier les paramètres. c Définissez une adresse IP statique pour le dispositif virtuel.

Suivant

- Si vous souhaitez configurer un déploiement autonome de vRealize Log Insight, reportez-vous à [Configurer un nouveau déploiement de Log Insight](#).

The vRealize Log Insight Web interface is available at `https://log-insight-host/` where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Rejoindre un déploiement existant

Une fois que vous avez déployé et configuré un nœud autonome vRealize Log Insight, vous pouvez déployer une nouvelle instance de vRealize Log Insight et l'ajouter au nœud existant afin de créer un cluster vRealize Log Insight.

vRealize Log Insight a la possibilité de monter en charge en utilisant plusieurs instances de dispositif virtuel dans des clusters. Grâce aux clusters, le débit d'ingestion évolue de manière linéaire, les performances des requêtes sont améliorées et l'ingestion est hautement disponible. En mode cluster, vRealize Log Insight fournit les nœuds maître et travailleurs. Ces deux types de nœuds sont responsables d'un sous-ensemble de données ; un nœud maître peut interroger tous les sous-ensembles de données et agréger les résultats.

Important Configurez au minimum trois nœuds dans un cluster vRealize Log Insight afin d'assurer la haute disponibilité de l'ingestion, de la configuration et de l'espace utilisateur.

Prérequis

- Dans vSphere Client, notez l'adresse IP du dispositif virtuel vRealize Log Insight travailleur.
- Vérifiez que vous disposez de l'adresse IP ou du nom de domaine du dispositif virtuel vRealize Log Insight maître.
- Vérifiez que vous disposez d'un compte d'administrateur sur le dispositif virtuel vRealize Log Insight maître.
- Vérifiez que les versions des nœuds maître et travailleurs de vRealize Log Insight sont synchronisées. N'ajoutez pas une ancienne version travailleur de vRealize Log Insight à une nouvelle version de nœud maître de vRealize Log Insight.
- Vous devez synchroniser l'heure sur le dispositif virtuel vRealize Log Insight avec un serveur NTP. Voir [Synchroniser l'heure sur le dispositif virtuel Log Insight](#).
- Pour obtenir des informations sur les versions d'explorateur prises en charge, reportez-vous aux [Notes de mise à jour de vRealize Log Insight](#).

Procédure

- 1 Utilisez un navigateur pris en charge pour accéder à l'interface utilisateur Web du vRealize Log Insight travailleur.

Le format de l'URL est `https://log_insight-host/`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight travailleur.

L'assistant de configuration initiale s'ouvre.

- 2 Cliquez sur **Rejoindre un déploiement existant**.
- 3 Entrez l'adresse IP ou le nom d'hôte du vRealize Log Insight maître, puis cliquez sur **Aller à**.

Le travailleur envoie au nœud vRealize Log Insight maître une demande pour rejoindre le déploiement existant.

4 Cliquez sur **Cliquez ici pour accéder à la page Gestion de cluster**.

5 Connectez-vous en tant qu'administrateur.

La page Cluster se charge.

6 Cliquez sur **Autoriser**.

Le travailleur rejoint le déploiement existant et vRealize Log Insight commence à fonctionner dans un cluster.

Suivant

- Pour ajouter un autre travailleur, déployez une nouvelle instance de vRealize Log Insight et ajoutez-la au cluster à l'aide de l'assistant de configuration.
- Reprenez la procédure pour ajouter au minimum deux nœuds travailleurs de vRealize Log Insight.

Supprimer un nœud travailleur d'un cluster vRealize Log Insight



Vous pouvez supprimer un nœud travailleur qui ne fonctionne plus correctement depuis un cluster vRealize Log Insight et l'ajouter à un différent cluster ou bien démarrer un déploiement autonome. Ne supprimez pas les nœuds travailleurs qui fonctionnent correctement depuis un cluster.

La suppression d'un nœud entraîne une perte de données. Si un nœud doit être supprimé, assurez-vous qu'il est d'abord sauvegardé. Évitez de supprimer des nœuds dans les 30 minutes suivant l'ajout de nouveaux nœuds.

Prérequis


Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Cluster**.
- 3 In the Workers table, find the node you want, click the pause icon,  and click **Continue**.

The node is now in maintenance mode.

Remarque A node in maintenance mode continues to receive logs.

- 4 Cliquez sur  pour supprimer le nœud.

vRealize Log Insight supprime le nœud du cluster et envoie une notification par e-mail.

Suivant

Accédez à l'interface utilisateur Web du nœud supprimé pour le configurer. Vous pouvez ajouter le nœud à un autre cluster vRealize Log Insight déjà créé ou démarrer un nouveau déploiement autonome.

Utilisation de l'équilibrage de charge intégrée

Vous pouvez activer l'équilibrage de charge intégrée (ILB) vRealize Log Insight sur un cluster vRealize Log Insight pour vous assurer que le trafic d'ingestion entrant est accepté par vRealize Log Insight même si certains nœuds vRealize Log Insight ne sont plus disponibles. Vous pouvez également configurer plusieurs adresses IP virtuelles.

Il est particulièrement recommandé d'activer l'équilibrage de charge intégré dans un environnement de cluster vRealize Log Insight pour équilibrer le trafic entre les nœuds d'un cluster et pour réduire la capacité administrative.

Remarque External load balancers are not suggested for use with vRealize Log Insight. Support will be removed in a later version.

Il est recommandé d'inclure l'équilibrage de charge intégré dans tous les déploiements, notamment les instances de nœud unique. Envoyez des requêtes et le trafic d'ingestion à l'équilibrage de charge intégré de sorte qu'un cluster puisse facilement être pris en charge à l'avenir si nécessaire.

L'équilibrage de charge intégré garantit que le trafic d'ingestion entrant est accepté par vRealize Log Insight, même si certains nœuds vRealize Log Insight ne sont plus disponibles. En outre, l'équilibrage de charge intégré homogénéise équitablement le trafic entrant entre les nœuds vRealize Log Insight disponibles. Utilisant à la fois l'interface utilisateur Web et l'ingestion (via Syslog ou l'API d'ingestion), les clients vRealize Log Insight doivent se connecter à vRealize Log Insight via l'adresse d'équilibrage de charge intégré.

L'équilibrage de charge intégré nécessite que tous les nœuds vRealize Log Insight résident sur le même réseau de couche 2, par exemple derrière le même commutateur, ou que chaque nœud soit en mesure d'envoyer des requêtes ARP aux autres nœuds et de recevoir les requêtes ARP envoyées par ceux-ci. L'adresse IP d'équilibrage de charge intégré doit être configurée de manière que tout nœud vRealize Log Insight puisse l'exploiter et recevoir du trafic pour elle. Par conséquent, l'adresse IP d'équilibrage de charge intégré réside généralement sur le même sous-réseau que l'adresse physique des nœuds vRealize Log Insight. Une fois l'adresse IP d'équilibrage de charge intégré configurée, essayez de lui envoyer un ping à partir d'un autre réseau pour vous assurer qu'elle est accessible.

Pour simplifier les modifications et les mises à niveau futures, vous pouvez faire pointer les clients vers un nom de domaine complet qui se résout en l'adresse IP d'équilibrage de charge intégré, au lieu de pointer directement vers celle-ci.

À propos de la configuration de Direct Server Return

L'équilibrage de charge de vRealize Log Insight utilise une configuration Direct Server Return (DSR). Dans DSR, tout le trafic entrant transite par le nœud vRealize Log Insight qui est le nœud d'équilibrage de charge actuel tandis que le trafic de retour est envoyé des serveurs vRealize Log Insight directement au client sans devoir transiter par le nœud de l'équilibrage de charge.

Adresses IP virtuelles multiples

Vous pouvez configurer plusieurs adresses IP virtuelles (vIP) pour l'équilibrage de charge intégrée. Vous pouvez également configurer une liste de balises statiques pour chaque adresse IP virtuelle, afin que chaque message de journal reçu de l'adresse IP virtuelle soit annoté avec les balises configurées.


Activer l'équilibrage de charge intégrée

Lorsque vous activez l'équilibrage de charge intégrée (ILB) de vRealize Log Insight sur un cluster vRealize Log Insight, vous pouvez configurer une ou plusieurs adresses IP virtuelles. Vous pouvez facultativement permettre aux utilisateurs d'accéder au cluster via un nom de domaine complet.

Prérequis

- Vérifiez que tous les nœuds vRealize Log Insight et l'adresse IP d'équilibrage de charge intégré spécifiée se trouvent sur le même réseau.
- Les nœuds maîtres et travailleurs vRealize Log Insight doivent être dotés des mêmes certificats. Dans le cas contraire, les agents vRealize Log Insight configurés pour se connecter par SSL rejettent la connexion. Lorsque vous téléchargez un certificat signé par une autorité de certification vers des nœuds maîtres ou travailleurs vRealize Log Insight, définissez le nom commun sur l'adresse IP d'équilibrage de charge intégré lors de la demande de génération de certificat. Reportez-vous à [Générer une demande de signature de certificat](#).
- You must synchronize the time on the vRealize Log Insight virtual appliance with an NTP server. See [Synchronize the Time on the Log Insight Virtual Appliance](#).

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Cluster**.
- 3 Sous Configuration, sélectionnez **Nouvelle adresse IP virtuelle** et entrez l'adresse IP virtuelle (vIP) à utiliser pour l'équilibrage de charge intégré.
- 4 (Facultatif) Pour configurer plusieurs adresses IP virtuelles, cliquez sur **Nouvelle adresse IP virtuelle** et entrez l'adresse IP. Vous pouvez choisir d'entrer le nom de domaine complet et des balises.
 - Chaque vIP doit se trouver dans le même sous-réseau qu'au moins une interface réseau sur chaque nœud et l'adresse IP virtuelle doit être disponible (non utilisée par une autre machine).

- Les balises vous permettent d'ajouter des champs avec des valeurs prédéfinies à des événements pour faciliter l'exécution d'une requête. Vous pouvez ajouter plusieurs balises séparées par des virgules. Tous les événements entrant dans le système via une adresse IP virtuelle sont marqués avec les balises des adresses IP virtuelles.
 - Vous pouvez configurer une liste de balises statiques (key=value) pour une adresse IP virtuelle d'équilibrage de charge intégrée, afin que chaque message de journal reçu de l'adresse IP virtuelle soit annoté avec les balises configurées.
- 5 (Facultatif) Pour permettre aux utilisateurs vRealize Log Insight d'accéder au cluster via un FQDN, faites pointer les clients vers le FQDN plutôt que directement vers l'adresse IP ILB configurée.
 - 6 Cliquez sur **Enregistrer**.

L'équilibrage de charge intégré est géré par un nœud dans le cluster vRealize Log Insight, déclaré leader de ce service. Le leader actuel est décrit par le texte (ILB) en regard du nœud.

Interroger les résultats des vérifications du cluster en production

Le service de vérification du cluster en production exécute régulièrement un ensemble de tests sur chaque nœud. Vous pouvez interroger les derniers résultats des vérifications du cluster en production à l'aide de l'interface de ligne de commande.

Par exemple, le service détermine si le cluster s'exécute et a été configuré comme prévu ou si des problèmes concernant l'intégration à d'autres systèmes se sont produits. Les vérifications supplémentaires sont énumérées ci-dessous.

- NTP est-il configuré dans un déploiement à plusieurs hôtes ?
- Active Directory est-il accessible (s'il est configuré actuellement) ?
- L'authentification d'Active Directory peut-elle se produire (si elle est configurée actuellement) ?
- Les hôtes Active Directory et les hôtes Kerberos sont-ils accessibles (si Active Directory est configuré actuellement) ?
- Le système s'exécute-t-il dans un déploiement à deux hôtes non pris en charge ?
- L'espace disponible dans /tmp est-il suffisant pour réaliser une mise à niveau ?
- L'espace disponible dans /storage/core est-il suffisant pour réaliser une mise à niveau ?
- L'hôte local est-il correctement placé dans /etc/hosts ?

Procédure

- 1 Sur la ligne de commande, établissez une connexion SSH au dispositif virtuel vRealize Log Insight, puis connectez-vous en tant qu'utilisateur racine.
- 2 Sur la ligne de commande, tapez `/usr/lib/loginsight/application/sbin/query-check-results.sh`, puis appuyez sur **Entrée**.

Ports et interfaces externes

vRealize Log Insight utilise des services, des ports et des interfaces externes spécifiques requis.

Ports de communication

vRealize Log Insight utilise les ports et les protocoles de communication énumérés dans cette rubrique. Les ports requis sont organisés selon qu'ils sont requis pour les sources, pour l'interface utilisateur, entre des clusters, pour les services externes, ou selon qu'ils peuvent être bloqués en toute sécurité par un pare-feu. Certains ports sont utilisés uniquement si vous activez l'intégration correspondante.

Remarque vRealize Log Insight ne prend pas en charge le clustering WAN (également appelé géoclustering, clustering haute disponibilité ou clustering distant). Tous les nœuds du cluster doivent être déployés dans le même réseau local de couche 2. En outre, les ports décrits dans cette section doivent être ouverts entre les nœuds pour garantir une bonne communication.

Le trafic réseau de vRealize Log Insight dispose de plusieurs sources.

Poste de travail administrateur	Machine utilisée par un administrateur système pour gérer le dispositif virtuel vRealize Log Insight à distance.
Poste de travail utilisateur	Machine sur laquelle un utilisateur vRealize Log Insight accède à l'interface Web de vRealize Log Insight à l'aide d'un navigateur.
Système envoyant des journaux	Point de terminaison qui envoie des journaux à vRealize Log Insight pour effectuer une analyse et une recherche. Les points de terminaison sont par exemple des hôtes ESXi, des machines virtuelles ou tout système doté d'une adresse IP.
Log Insight Agents	Agent qui réside sur une machine Windows ou Linux et envoie des journaux et des événements du système d'exploitation à vRealize Log Insight par des API.
Dispositif vRealize Log Insight	Tout dispositif virtuel vRealize Log Insight (maître ou travailleur) sur lequel résident les services vRealize Log Insight. Le système d'exploitation de base du dispositif est SUSE 11 SP3.

Ports requis pour les sources envoyant des données

Les ports suivants doivent être ouverts pour le trafic réseau depuis des sources qui envoient des données à vRealize Log Insight, pour les connexions depuis l'extérieur du cluster et pour les connexions équilibrées en charge entre les nœuds de cluster.

Source	Destination	Port	Protocole	Description du service
Système envoyant des journaux	Dispositif vRealize Log Insight	514	TCP, UDP	Trafic syslog sortant configuré en tant que destination de redirecteur
Système envoyant des journaux	Dispositif vRealize Log Insight	1514, 6514	TCP	Données Syslog via SSL
Agents vRealize Log Insight	Dispositif vRealize Log Insight	9000	TCP	API Ingestion de Log Insight
Agents vRealize Log Insight	Dispositif vRealize Log Insight	9543	TCP	API Ingestion de Log Insight par SSL

Ports requis pour l'interface utilisateur

Les ports suivants doivent être ouverts pour le trafic réseau qui doit utiliser l'interface utilisateur vRealize Log Insight, pour les connexions à l'extérieur du cluster et pour les connexions équilibrées en charge entre les nœuds de cluster.

Source	Destination	Port	Protocole	Description du service
Poste de travail administrateur	Dispositif vRealize Log Insight	22	TCP	SSH : connectivité Secure Shell
Poste de travail utilisateur	Dispositif vRealize Log Insight	80	TCP	HTTP : interface Web
Poste de travail utilisateur	Dispositif vRealize Log Insight	443	TCP	HTTPS : interface Web

Ports requis entre des nœuds de clusters

Les ports suivant doivent uniquement être ouverts sur un nœud maître vRealize Log Insight pour un accès réseau depuis des nœuds travailleurs, pour une sécurité optimale. Ces ports s'ajoutent aux ports utilisés pour les sources et le trafic d'interface utilisateur qui sont équilibrés en charge entre les nœuds de cluster.

Source	Destination	Port	Protocole	Description du service
Dispositif vRealize Log Insight	Dispositif vRealize Log Insight	7000	TCP	Requête et réplication Cassandra
Dispositif vRealize Log Insight	Dispositif vRealize Log Insight	9042	TCP	Service Cassandra pour les clients de protocole natif
Dispositif vRealize Log Insight	Dispositif vRealize Log Insight	9160	TCP	Service Cassandra pour les clients Thrift
Dispositif vRealize Log Insight	Dispositif vRealize Log Insight	59778, 16520-16580	TCP	Service vRealize Log Insight Thrift

Ports requis pour les services externes

Les ports suivants doivent être ouverts pour le trafic de réseau sortant depuis des nœuds de cluster de vRealize Log Insight vers des services distants.

Source	Destination	Port	Protocole	Description du service
Dispositif vRealize Log Insight	serveur NTP	123	UDP	NTPD : permet la synchronisation de l'heure NTP Remarque Le port est ouvert uniquement si vous décidez d'utiliser la synchronisation de l'heure NTP
Dispositif vRealize Log Insight	Serveur de messagerie	25	TCP	SMTP : service de messagerie pour alertes sortantes
Dispositif vRealize Log Insight	Serveur de messagerie	465	TCP	SMTPS : service de messagerie via SSL pour alertes sortantes
Dispositif vRealize Log Insight	Serveur DNS	53	TCP, UDP	DNS : service de résolution de noms
Dispositif vRealize Log Insight	Serveur AD	389	TCP, UDP	Active Directory
Dispositif vRealize Log Insight	Serveur AD	636	TCP	Active Directory via SSL
Dispositif vRealize Log Insight	Serveur AD	3268	TCP	Catalogue global Active Directory
Dispositif vRealize Log Insight	Serveur AD	3269	TCP	Protocole SSL de catalogue global Active Directory
Dispositif vRealize Log Insight	Serveur AD	88	TCP, UDP	Kerberos

Source	Destination	Port	Protocole	Description du service
Dispositif vRealize Log Insight	vCenter Server	443	TCP	Service Web vCenter Server
Dispositif vRealize Log Insight	Dispositif vRealize Operations Manager	443	TCP	Service Web vRealize Operations
Dispositif vRealize Log Insight	Gestionnaire de journaux tiers	514	TCP, UDP	Données Syslog
Dispositif vRealize Log Insight	Gestionnaire de journaux tiers	9000	CFAPI	Trafic d'API Log Insight Ingestion (CFAPI) sortant configuré en tant que destination de redirecteur
Dispositif vRealize Log Insight	Gestionnaire de journaux tiers	9543	CFAPI	Trafic d'API Log Insight Ingestion (CFAPI) sortant configuré en tant que destination de redirecteur avec chiffrement (SSL/TLS)

Ports pouvant être bloqués

Les ports suivants sont ouverts, mais ne sont pas utilisés par vRealize Log Insight. Ces ports peuvent être bloqués en toute sécurité par un pare-feu.

Destination	Port	Protocole	Description du service
Dispositif vRealize Log Insight	111	TCP, UDP	Service RPCbind qui convertit les numéros du programme RPC en adresses universelles
Service Tomcat de dispositif vRealize Log Insight	9007	TCP	Services Tomcat

Surveiller l'état des agents Windows et Linux de vRealize Log Insight

7

Vous pouvez surveiller l'état des agents Windows et Linux de vRealize Log Insight et afficher les statistiques actuelles à propos de leur fonctionnement.


Seuls les agents qui sont configurés pour envoyer des données via CFAPI apparaissent dans la page Agents. Les agents qui sont configurés pour envoyer des données via Syslog apparaissent dans la page Hôtes, tout comme les autres sources Syslog.

Remarque Si vous modifiez une adresse IP de l'hôte pour un serveur vRealize Log Insight dans la configuration de l'agent, l'agent réinitialise les statistiques de page à zéro.

Prérequis

Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the **View Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Sous Gestion, cliquez sur **Agents**.

Suivant

Vous pouvez utiliser les informations dans la page Agents pour surveiller le fonctionnement des agents Windows et Linux de vRealize Log Insight installés.

Activer la mise à jour automatique des agents à partir du serveur



Vous pouvez activer la mise à jour automatique de tous les agents à partir du serveur vRealize Log Insight.


La mise à jour automatique applique la dernière mise à jour disponible à tous les agents connectés au serveur. Vous pouvez désactiver la fonctionnalité de mise à jour automatique pour des serveurs spécifiques en modifiant le fichier `liagent.ini` de l'agent. Pour plus d'informations, consultez *Utilisation d'agents vRealize Log Insight*.

La mise à jour automatique est désactivée pour le serveur par défaut.

Prérequis

Elle s'applique aux agents qui sont à l'état Actif et dont la version est 4.3 ou ultérieure.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Cliquez sur **Agents** dans le menu situé à gauche.
- 3 Cliquez sur la commande à bascule pour **Activer la mise à jour pour tous les agents** sur la page Agents.

Les agents connectés à ce serveur sont mis à jour dès qu'une mise à jour est disponible.

Utilisation des groupes d'agents

En utilisant un serveur vRealize Log Insight, vous pouvez configurer des agents à partir de l'interface utilisateur de l'application. Les agents interrogent le serveur vRealize Log Insight de façon régulière pour déterminer si de nouvelles configurations sont disponibles.

Vous pouvez regrouper les agents qui nécessitent la même configuration. Vous pouvez par exemple regrouper tous les agents vRealize Log Insight Windows séparément des agents vRealize Log Insight Linux.

Dans le menu **Tous les agents**, les groupes d'agents existants des packs de contenu sont listés automatiquement. Les agents listés sont associés aux packs de contenu que vous avez déjà installés (par exemple, le pack de contenu vSphere) et qui utilisent des groupes d'agents.

Les groupes du pack de contenu sont en lecture seule.

Seules les sections de configuration commençant par `[winlog]`, `[filelog]` et `[parser]` sont utilisées dans les packs de contenu. Les autres sections ne sont pas exportées dans un pack de contenu. Seuls les commentaires sur une ligne (les lignes commençant par un point-virgule « ; ») sous les sections `[winlog]`, `[filelog]` et `[parser]` sont conservés dans un pack de contenu.

Consultez *Utilisation d'agents vRealize Log Insight* pour plus d'informations sur la configuration d'agents, notamment la fusion de configurations entre les configurations locale et côté serveur.

- [Fusion de la configuration d'un groupe d'agents](#)

Avec les groupes d'agents, les agents peuvent faire partie de plusieurs groupes et peuvent appartenir au groupe par défaut *Tous les agents*, pour permettre une configuration centralisée.

- [Créer un groupe d'agents](#)

Vous pouvez créer un groupe d'agents qui seront configurés avec les mêmes paramètres.

- [Modifier un groupe d'agents](#)

Vous pouvez modifier le nom et la description d'un groupe d'agents, ainsi que les filtres et la configuration.

- [Ajouter un groupe d'agents de pack de contenu en tant que groupe d'agents](#)

Vous pouvez ajouter un groupe d'agents qui est défini comme appartenant à un pack de contenu à vos groupes actifs et appliquer la configuration de l'agent à ce groupe.

- [Supprimer un groupe d'agents](#)

Vous pouvez supprimer un groupe d'agent pour le retirer de la liste des groupes actifs.

Fusion de la configuration d'un groupe d'agents

Avec les groupes d'agents, les agents peuvent faire partie de plusieurs groupes et peuvent appartenir au groupe par défaut *Tous les agents*, pour permettre une configuration centralisée.

La fusion se produit côté serveur et la configuration résultante est fusionnée avec la configuration côté agent. La configuration fusionnée est régie par les règles suivantes.

- Les configurations de groupes individuels ont priorité sur les paramètres du groupe *Tous les agents*.
- La configuration du groupe *Tous les agents* a préséance sur la configuration locale.
- Vous ne pouvez pas configurer des sections en utilisant le même nom dans différents groupes à l'exception des groupes *Tous les agents*. Cependant, les sections des groupes individuels ont une priorité plus élevée.

Remarque Pour éviter la perte d'agents, les paramètres **hostname** et **port** d'une configuration d'agent ne peuvent pas être modifiés centralement sur le serveur.

La configuration fusionnée est stockée dans le fichier `liagent-effective.ini` côté agent.


Créer un groupe d'agents

Vous pouvez créer un groupe d'agents qui seront configurés avec les mêmes paramètres.

Prérequis

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
 - 2 Sous Gestion, cliquez sur **Agents**.
 - 3 Dans le menu **Tous les agents**, cliquez sur **Nouveau groupe**.
 - 4 Entrez un nom unique et une description pour le groupe d'agents et cliquez sur **Nouveau groupe**.
Le groupe d'agents est créé et apparaît dans la liste **Tous les agents**, mais il n'est pas enregistré.
 - 5 Spécifiez un ou plusieurs des filtres suivants pour le groupe d'agents.
Les filtres peuvent contenir des caractères spéciaux, tels que * et ?.
- adresse IP
 - nom d'hôte

- version
- SE

Par exemple, vous pouvez sélectionner le filtre SE contains et spécifier la valeur windows afin d'identifier tous vos agents Windows pour la configuration.

- 6 Spécifiez les valeurs de la configuration de l'agent dans la zone Configuration de l'agent et cliquez sur **Enregistrer le nouveau groupe**.

La configuration de l'agent est appliquée après le prochain intervalle d'interrogation.


Modifier un groupe d'agents

Vous pouvez modifier le nom et la description d'un groupe d'agents, ainsi que les filtres et la configuration.

Prérequis

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Sous Gestion, cliquez sur **Agents**.
- 3 Dans le menu **Tous les agents**, sélectionnez le nom du groupe d'agents approprié et cliquez sur l'icône en forme de crayon pour le modifier.
- 4 Apportez vos modifications.

Élément à modifier	Action
Nom et description	Effectuez les modifications nécessaires et cliquez sur Enregistrer .
Filtres ou Configuration	Effectuez les modifications nécessaires et cliquez sur Enregistrer le groupe .


Ajouter un groupe d'agents de pack de contenu en tant que groupe d'agents

Vous pouvez ajouter un groupe d'agents qui est défini comme appartenant à un pack de contenu à vos groupes actifs et appliquer la configuration de l'agent à ce groupe.

Prérequis

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Sous Gestion, cliquez sur **Agents**.
- 3 Dans le menu **Tous les agents**, sélectionnez un modèle d'agent pour la liste des modèles disponibles.
- 4 Cliquez sur **Copier le modèle** pour copier le groupe d'agents de pack de contenu vers vos groupes actifs.
- 5 Cliquez sur **Copier**.
- 6 Sélectionnez les champs requis et cliquez sur **Enregistrer le nouveau groupe**.

Le groupe d'agents de pack de contenu est ajouté à vos groupes actifs et les agents sont configurés en fonction des filtres que vous avez spécifiés.


Supprimer un groupe d'agents

Vous pouvez supprimer un groupe d'agent pour le retirer de la liste des groupes actifs.

Prérequis

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Sous Gestion, cliquez sur **Agents**.
- 3 Dans le menu **Tous les agents**, sélectionnez le nom d'un groupe d'agents à supprimer en cliquant sur l'icône X située à côté de son nom.
- 4 Cliquez sur **Supprimer**.

Le groupe d'agent est supprimé des groupes actifs.

Configuration et utilisation de vRealize Log Insight Importer

10

vRealize Log Insight Importer est un utilitaire de ligne de commande servant à importer des journaux hors ligne de données historiques de machines locales vers le serveur vRealize Log Insight.

vRealize Log Insight est un outil d'analyse de journaux en temps réel qui envoie des événements Syslog ou des événements d'agent à vRealize Log Insight, mais vous devrez éventuellement parfois importer des journaux ayant été collectés antérieurement. À l'aide de vRealize Log Insight Importer, vous pouvez importer des bundles de support et des journaux archivés pour ingérer des données ayant été collectées sur une période donnée. Vous pouvez analyser des journaux à partir de bundles de support collectés auprès de vRealize Log Insight ou de n'importe quel produit VMware.

vRealize Log Insight Importer offre les fonctionnalités et caractéristiques ci-dessous.

- vRealize Log Insight Importer envoie des données sur l'API Ingestion.
- Il prend en charge la collecte de journaux, y compris la collecte de répertoires récursifs.
- L'importateur peut lire les données de fichiers d'archives aux formats zip, tar ou gz.
- Vous pouvez spécifier que les données sont lues de manière récursive à partir d'une archive imbriquée (par ex., un fichier zip imbriqué), ou spécifier un répertoire au sein d'une archive.
- 7-Zip n'est pas pris en charge.

Utilisation de l'importateur de vRealize Log Insight

Assurez-vous que vRealize Log Insight a accès au serveur NFS sur lequel les données archivées sont stockées. Si le serveur NFS devient inaccessible en raison d'une panne réseau ou d'erreurs sur le serveur NFS, l'importation des données archivées peut échouer. N'oubliez pas que les restrictions suivantes s'appliquent lorsque vous utilisez vRealize Log Insight Importer.

Lorsque des journaux sont extraits d'un bundle au cours de l'ingestion, un nom de bundle de journaux est automatiquement déterminé et ajouté sous forme de balise de bundle à tous les journaux extraits. Le nom de la balise est le nom de fichier du journal ou le nom de répertoire en cas de sources de répertoire. Les balises de bundle différencient les bundles sur un serveur vRealize Log Insight.

Cette balise remplace les balises avec le même nom spécifiées dans le fichier manifeste. La balise peut être remplacée par des balises de ligne de commande qui utilisent le même nom.

Les limitations suivantes s'appliquent :

- vRealize Log Insight Importer ne vérifie pas l'espace disque disponible sur le dispositif virtuel vRealize Log Insight. L'importation des fichiers journaux archivés peut donc échouer si le dispositif virtuel ne dispose plus d'espace disque.
- vRealize Log Insight n'affiche pas les informations de progression lors des importations de journaux. Lorsqu'une importation de données archivées est en cours, vous ne pouvez pas déduire de la sortie de la console le temps restant avant la fin de l'importation ou le volume de données déjà importées.

Systèmes d'exploitation pris en charge

vRealize Log Insight Importer est pris en charge sur les systèmes d'exploitation suivants :

- Windows 32 bits et 64 bits
- Linux 32 bits et 64 bits

La version Linux ne fonctionne pas sur un système Apple Macintosh.

Ce chapitre aborde les rubriques suivantes :

- [À propos du fichier de manifeste de vRealize Log Insight Importer](#)
- [Installer, configurer et exécuter vRealize Log Insight Importer](#)
- [Exemples de configuration de fichier de manifeste vRealize Log Insight Importer](#)
- [Paramètres de configuration de vRealize Log Insight Importer](#)

À propos du fichier de manifeste de vRealize Log Insight Importer

vRealize Log Insight Importer utilise un fichier de configuration de manifeste pour déterminer le format du journal et pour spécifier l'emplacement des données à importer. Le fichier de manifeste a le même format que le fichier de configuration `liagent.ini` et présente une structure similaire.

Vous pouvez créer vos propres fichiers de manifeste pour importer des fichiers journaux arbitraires. Bien que la création d'un fichier de manifeste soit facultative, si vous utilisez un fichier de manifeste, vous n'avez pas besoin de connaître le chemin d'accès absolu aux fichiers de données.

Si vous ne créez pas de fichier de manifeste, vRealize Log Insight Importer utilise le manifeste par défaut qui collecte tous les fichiers `.txt` et `.log` (`include=*.log*;*.txt*`) et applique l'analyseur automatique (extrait horodatage + kvp) aux journaux extraits.

Si le fichier de configuration `liagent.ini` est utilisé comme fichier de manifeste, vRealize Log Insight Importer extrait uniquement les sections `[filelog]` comme manifeste. Toutes les options de la section `[filelog]` sont prises en charge dans vRealize Log Insight Importer.

Pour découvrir d'autres options prises en charge dans la section `[filelog]` et des exemples de configuration, reportez-vous à la documentation de l'agent vRealize Log Insight dans le *Guide d'administration des agents vRealize Log Insight*.

Pour créer un fichier de manifeste

Vous pouvez copier et coller le contenu du fichier de configuration de l'agent dans un nouveau fichier .txt. Pour identifier un chemin d'accès dynamique, supprimez la barre oblique (« / ») à gauche du chemin du répertoire.

Spécification du chemin du répertoire

Le répertoire spécifié dans la section [filelog] peut être relatif à la source ou absolu. Pour spécifier un chemin relatif, n'ajoutez pas la première barre oblique sous Linux, sinon le chemin d'accès sera considéré par vRealize Log Insight Importer comme étant absolu.

Pour indiquer des modèles de noms dans la valeur de la clé du répertoire, vous pouvez utiliser les caractères * et **.

- Utilisez * comme espace réservé d'un répertoire unique. Utilisez-le pour indiquer un niveau d'imbrication avec un nom de dossier arbitraire. Par exemple, utilisez `directory = log_folder_*` pour indiquer un dossier qui commence par la chaîne `log_folder_`.
- Utilisez ** pour indiquer un niveau arbitraire d'imbrication avec un nom de dossier. Par exemple, vous pouvez utiliser `directory = **/log` pour indiquer un dossier portant le nom `log` à tout niveau d'imbrication dans le répertoire source.

Installer, configurer et exécuter vRealize Log Insight Importer

Vous pouvez installer vRealize Log Insight Importer sur Windows et Linux. Vous pouvez également installer vRealize Log Insight Importer sur un serveur vRealize Log Insight et l'exécuter depuis le serveur.

Prérequis

- Vérifiez que vous pouvez accéder au site de [téléchargement VMware](#) pour télécharger vRealize Log Insight Importer.
- Lisez [À propos du fichier de manifeste de vRealize Log Insight Importer](#) et créez un fichier manifeste à utiliser avec l'importateur. Pour plus d'informations, consultez [Exemples de configuration de fichier de manifeste vRealize Log Insight Importer](#).
- Consultez [Paramètres de configuration de vRealize Log Insight Importer](#) pour identifier les paramètres requis et facultatifs disponibles.
- Si vous utilisez le paramètre `honor_timestamp`, vérifiez que vous disposez des informations d'identification de connexion appropriées.
- Si vous importez un bundle de support, vous devez configurer le paramètre `honor_timestamp`, ainsi que le nom d'utilisateur et le mot passe.

Procédure

- 1 Téléchargez le module d'installation de vRealize Log Insight Importer sur le site de [téléchargement de VMware](#), puis installez l'outil sur votre système. Les modules d'installation incluent le programme d'installation MSI pour Windows et les modules d'installation POSIX (RPM, DEB et BIN) pour Linux.

L'outil vRealize Log Insight Importer est installé aux emplacements suivants.

Système d'exploitation	Nom de fichier	Emplacement d'installation
Windows	loginsight-importer.exe	C:\Program Files (x86)\VMware\Log Insight Importer
Linux	loginsight-importer	/usr/lib/loginsight-importer

Remarque

- Après l'installation, le répertoire d'installation de l'importateur est ajouté à la variable d'environnement PATH sur Windows, et un lien symbolique vers l'exécutable loginsight-importer est ajouté à /usr/bin/ sur Linux. Le client peut ainsi appeler loginsight-importer à partir du shell sans spécifier de préfixe de chemin d'accès.
- Lorsque vous installez vRealize Log Insight Importer, plusieurs fichiers manifestes de produit VMware sont également installés. Vous pouvez utiliser ces fichiers ou les modifier selon vos besoins lors de l'exécution de vRealize Log Insight Importer. Ces fichiers manifestes sont situés dans C:\Program Files (x86)\VMware\Log Insight Importer\Manifests pour Windows et dans /usr/lib/loginsight-importer/manifests pour Linux.
- Si vous désinstallez le module .bin, vous devez également supprimer le lien symbolique /usr/bin/loginsight_importer.

- 2 Démarrez l'outil vRealize Log Insight Importer en entrant la commande suivante à l'invite de commande.

```
/usr/bin/loginsight-importer.exe
```

- 3 Entrez le nom du fichier de manifeste en réponse à l'invite.
- 4 Définissez les paramètres de configuration et appuyez sur **Entrée**.

vRealize Log Insight Importer commence à extraire les entrées de journaux à partir des répertoires spécifiés dans les paramètres. Le nombre total de fichiers traités, de messages de journaux extraits, de messages de journaux envoyés et la durée d'exécution s'affichent.

- 5 Une fois l'importation terminée, appuyez sur **Ctrl+C** sous Windows ou Linux pour quitter l'outil.

Suivant

Dans l'onglet Analyse interactive de vRealize Log Insight, vous pouvez actualiser l'affichage pour répertorier les événements de journaux importés. Si vous avez importé un bundle de support et utilisé le paramètre honor_timestamp, le tableau de bord doit également afficher les événements dans le temps.

Exemples de configuration de fichier de manifeste vRealize Log Insight Importer

Les exemples de fichiers de manifeste vRealize Log Insight Importer fournissent des exemples de configuration de paramètres.

La valeur de la clé du répertoire doit être relative à la source ou absolue. L'exemple suivant montre comment collecter les journaux des fichiers portant une extension `.log` se trouvant à deux niveaux en-dessous du répertoire source et dont le nom du dernier dossier se termine par la chaîne `_log`.

```
[filelog|importer_test]
directory=*\*_log
include=*.log
event_marker=^\\d{4}-\\d{2}-\\d{2} \\d{2}:\\d{2}:\\d{2} [A-Z]{4} LOG
```

L'exemple suivant montre comment collecter tous les fichiers portant l'extension `.log` de tous les sous-dossiers du répertoire source, ce dernier inclus.

```
[filelog|sbimporter_test_channel]
directory = **
include = *.log
```

L'exemple suivant montre comment collecter les journaux de tous les fichiers du répertoire source (mais pas de ses sous-dossiers) à l'exception des fichiers portant l'extension `.ini`. Nous interprétons les fichiers comme ayant le codage UTF-16LE.

```
[filelog|quotes_channe3]
directory=
charset=UTF-16LE
exclude=*.ini
tags={"Provider" : "Apache"}
```

L'exemple suivant montre comment collecter les journaux de tous les fichiers portant l'extension `.log` dans le répertoire source (mais pas des sous-dossiers). L'horodatage des événements est analysé dans le fichier journal à l'aide de l'analyseur CLF (Common Log Format) et l'horodatage historique extrait est appliqué. Le format du journal analysé par l'analyseur CLF est `2015-03-25 22:11:46,786 | DEBUG | pool-jetty-76 | AuthorizationMethodInterceptor | Authorizing method: public abstract.`

```
[filelog|vcd-container-debug]
directory=
include=*.log
parser=vcd

[parser|vcd]
base_parser=clf
format=%Y-%m-%d %H:%M:%S%f}t %M
```


Paramètres de configuration de vRealize Log Insight Importer

La configuration de vRealize Log Insight Importer inclut des paramètres requis et facultatifs.

Paramètres requis	Description
<code>--source <chemin></code>	Spécifie le chemin d'accès au répertoire du bundle de support ou le chemin d'accès à l'archive zip, gzip ou tar du bundle. La valeur est ajoutée à tous les messages envoyés comme valeur de la balise <code>bundle</code> .
<code>--server <nom d'hôte></code>	Nom d'hôte ou adresse IP du serveur de destination.
Options	Description
<code>--port <port></code>	Port de la connexion. S'il n'est pas défini, le port 9000 est utilisé pour les connexions autres que SSL et le port 9543 est utilisé pour une connexion SSL.
<code>--logdir <chemin></code>	Spécifie le chemin d'accès au répertoire des journaux. S'il n'est pas défini, le chemin d'accès est : <code>\$ (LOCALAPPDATA)\VMware\Log Insight Importer\log</code> sous Windows et <code>~/loginsight-importer/log</code> sous Linux.
<code>--manifest <file-path></code>	Spécifie le chemin d'accès au fichier de manifeste (format .ini). S'il n'est pas défini, le fichier <code>importer.ini</code> du répertoire source est utilisé. Si le fichier <code>importer.ini</code> n'existe pas ou est introuvable dans le répertoire source, vRealize Log Insight Importer applique le manifeste par défaut (codé en dur), collecte tous les fichiers <code>.txt</code> et <code>.log</code> (<code>include=*.log*;*.txt*</code>) et applique également l'analyseur automatique (extrait l'horodatage + kvp).
<code>--no_ssl</code>	Ne pas utiliser SSL pour les connexions. Ce paramètre ne doit pas être défini pour les connexions authentifiées (par exemple si <code>--honor_timestamp</code> est employé).
<code>--ssl_ca_path <chemin></code>	Chemin d'accès au fichier du bundle de certificats racines.
<code>--tags <balises></code>	Définir les balises pour tous les événements envoyés. Par exemple, <code>--tags "{ \"balise1\" : \"valeur1\", \"balise2\" : \"valeur2\" }"</code> Remarque L'option <code>tags</code> peut accepter <code>hostname</code> comme nom de balise. La valeur de la balise <code>hostname</code> de la ligne de commande est utilisée à la place du nom de domaine complet de la machine émettrice comme valeur du champ <code>hostname</code> pour tous les événements extraits par vRealize Log Insight Importer. C'est le contraire du paramètre <code>tags</code> du fichier de manifeste et des champs extraits par les analyseurs, qui ignorent le champ <code>hostname</code> . Le nom d'un bundle de journaux, un nom de fichier ou un nom de répertoire en cas de sources de répertoire, est automatiquement déterminé et ajouté en tant que balise de <code>bundle</code> à tous les journaux extraits à partir de ce bundle spécifique lors de l'ingestion. Cette balise vous permet de différencier les bundles dans vRealize Log Insight Server. Une balise de <code>bundle</code> remplace les balises avec le même nom dans le fichier manifeste. Elle peut cependant être remplacée par des balises de ligne de commande, s'il en existe une avec le nom <code>bundle</code> .
<code>--username <nom d'utilisateur></code>	Nom d'utilisateur pour l'authentification. Requis si <code>--honor_timestamp</code> est défini.
<code>--password <mot de passe></code>	Mot de passe pour l'authentification. Requis si <code>--honor_timestamp</code> est défini. La paire <code>username/password</code> désactive le décalage de temps autorisé sur le serveur vRealize Log Insight afin de rendre possible l'importation des données avec un horodatage historique.

Options	Description
<code>--honor_timestamp</code>	<p>Applique l'horodatage extrait. Les analyseurs configurés extraient l'horodatage des entrées de journal et <code>--honor_timestamp</code> applique l'horodatage extrait.</p> <ul style="list-style-type: none"> ■ Si l'horodatage est extrait à l'aide d'analyseurs configurés, cet horodatage sera appliqué aux événements. ■ En présence d'un événement dans le fichier journal, sans horodatage extrait, l'horodatage extrait de l'événement précédent du même fichier journal sera appliqué. ■ Si aucun horodatage n'est trouvé ou analysé dans le fichier, la valeur MTIME du fichier journal sera appliquée comme horodatage. <p>Remarque Si aucun fichier de manifeste n'a été fourni, le manifeste codé en dur par défaut que vRealize Log Insight Importer utilisera dispose de l'analyseur de journaux automatique activé. Dans ce cas, vRealize Log Insight Importer extrait l'horodatage des entrées de journal si le paramètre <code>--honor_timestamp</code> est utilisé.</p>
<code>--debug_level <1 2></code>	Augmente le niveau de détail du fichier journal. Cette valeur ne doit être modifiée que lors d'un dépannage. Dans des conditions normales, cet indicateur ne doit pas être utilisé.
<code>--help</code>	Afficher l'aide et quitter.

Surveillance de vRealize Log Insight

11

Vous pouvez surveiller le dispositif virtuel de vRealize Log Insight et les hôtes et appareils qui envoient les événements de journaux vers vRealize Log Insight.

Ce chapitre aborde les rubriques suivantes :

- [Vérifier la santé du dispositif virtuel vRealize Log Insight](#)
- [Surveiller les hôtes qui envoient des événements de journaux](#)


Vérifier la santé du dispositif virtuel vRealize Log Insight

Vous pouvez vérifier les ressources disponibles et les requêtes actives sur le dispositif virtuel vRealize Log Insight ainsi que consulter les statistiques actuelles sur le fonctionnement de vRealize Log Insight.

Prérequis

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **System Monitor**.
- 3 Si vRealize Log Insight s'exécute en tant que cluster, cliquez sur **Afficher les ressources de** et choisissez le nœud à surveiller.

- 4 Cliquez sur les boutons de la page Surveillance du système pour afficher les informations qui vous intéressent.

Option	Description
Ressources	Affichez des informations sur l'utilisation de la CPU, de la mémoire, des IOPS (en lecture et en écriture) et du stockage sur le dispositif virtuel vRealize Log Insight. Les diagrammes situés à droite représentent les données d'historique des dernières 24 heures ; ils sont actualisés toutes les cinq minutes. Les diagrammes situés à gauche affichent les informations des cinq dernières minutes ; ils sont actualisés toutes les trois secondes.
Requêtes actives	Affichez des informations sur les requêtes actives dans vRealize Log Insight.
Statistiques	Affichez les statistiques concernant les taux et les opérations d'ingestion de journaux. Pour afficher des statistiques plus détaillées, cliquez sur Afficher des statistiques avancées .

Suivant

Vous pouvez utiliser les informations de la page Surveillance du système pour gérer les ressources du dispositif virtuel vRealize Log Insight.

Surveiller les hôtes qui envoient des événements de journaux


Vous pouvez afficher la liste de tous les hôtes et périphériques qui envoient des événements de journaux à vRealize Log Insight et les surveiller.

Les entrées des tables d'hôtes expirent trois mois après le dernier événement ingéré.

Prérequis

Verify that you are logged in to the vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Sous Gestion, cliquez sur **Hôtes**.

Remarque Si vous avez configuré vCenter Server de manière à envoyer des événements et des alarmes, mais n'avez pas configuré les différents hôtes ESXi pour envoyer des journaux, la colonne Nom d'hôte répertorie vCenter Server et les différents hôtes ESXi en tant que source au lieu de ne répertorier que le système vCenter Server.

Intégration de vRealize Log Insight à des produits VMware

12

vRealize Log Insight peut être intégré à d'autres produits VMware dans le but d'utiliser les données de journaux et d'événements et d'améliorer la visibilité des événements se produisant dans votre environnement virtuel.

Intégration à VMware vSphere

Les utilisateurs Admin vRealize Log Insight peuvent configurer vRealize Log Insight de façon à ce qu'il se connecte aux systèmes vCenter Server toutes les deux minutes et collecte les données d'événements, d'alarmes et de tâches de ces systèmes vCenter Server. En outre, vRealize Log Insight peut configurer des hôtes ESXi via vCenter Server. Reportez-vous à [Connecter vRealize Log Insight à un environnement vSphere](#).

Intégration à VMware vRealize Operations Manager

Vous pouvez intégrer vRealize Log Insight au vApp vRealize Operations Manager et à la version installable de vRealize Operations Manager. Pour l'intégrer à la version installable, vous devez apporter des modifications supplémentaires à la configuration de vRealize Operations Manager. Pour plus d'informations sur la configuration de la version installable de vRealize Operations Manager dans le but de l'intégrer à vRealize Log Insight, reportez-vous au *Guide de démarrage de Log Insight*.

Il existe deux manières pour intégrer vRealize Log Insight à vRealize Operations Manager.

Événements de notification

Les utilisateurs Admin vRealize Log Insight peuvent configurer vRealize Log Insight pour l'envoi d'événements de notification à vRealize Operations Manager à partir des requêtes que vous créez. Reportez-vous à [Configurer vRealize Log Insight pour envoyer des événements de notification à vRealize Operations Manager](#).

Lancement contextuel

Le lancement contextuel est une fonctionnalité de vRealize Operations Manager qui vous permet, dans un contexte particulier, de lancer une application externe via URL. Le contexte en question est défini par l'élément de l'interface utilisateur actif et par l'objet sélectionné. Avec le lancement contextuel, l'adaptateur

vRealize Log Insight ajoute des éléments de menu à différentes vues dans l'interface utilisateur personnalisée et dans l'interface utilisateur vSphere de vRealize Operations Manager. Reportez-vous à [Activer le lancement contextuel de vRealize Log Insight dans vRealize Operations Manager](#).

Remarque Les événements de notification ne dépendent pas de la configuration du lancement contextuel. Des événements de notification peuvent être envoyés de vRealize Log Insight vers vRealize Operations Manager, même si la fonctionnalité de lancement contextuel n'est pas activée.

Si l'environnement change, les utilisateurs Admin de vRealize Log Insight peuvent modifier, ajouter ou supprimer des systèmes vSphere à partir de vRealize Log Insight, modifier ou supprimer l'instance de vRealize Operations Manager à laquelle sont envoyées les notifications d'alerte et modifier les mots de passe utilisés pour la connexion aux systèmes vSphere et à vRealize Operations Manager.

Ce chapitre aborde les rubriques suivantes :

- [Connecter vRealize Log Insight à un environnement vSphere](#)
- [Configurer vRealize Log Insight pour l'extraction des événements, des tâches et des alarmes d'une instance de vCenter Server](#)
- [Utilisation de vRealize Operations Manager avec vRealize Log Insight](#)
- [Pack de contenu de vRealize Operations Manager pour vRealize Log Insight](#)

Connecter vRealize Log Insight à un environnement vSphere

Avant de configurer vRealize Log Insight pour la collecte des données d'alarmes, d'événements et de tâches issues de l'environnement vSphere, vous devez connecter vRealize Log Insight à un ou à plusieurs systèmes vCenter Server.

vRealize Log Insight peut collecter deux types de données des instances de vCenter Server et des hôtes ESXi gérés par ces dernières.

- Les événements, les tâches et les alertes sont des données structurées qui ont une signification particulière. Lorsque vRealize Log Insight est configuré à cette intention, les événements, les tâches et les alertes sont extraits des instances de vCenter Server inscrites.
- Les journaux contiennent des données non structurées qui peuvent être analysées dans vRealize Log Insight. Les hôtes ESXi ou les instances de vCenter Server Appliance peuvent transmettre leurs journaux vers vRealize Log Insight à travers Syslog.

Prérequis


- Vérifiez que vos informations d'identification d'utilisateur disposent des privilèges suffisants pour configurer correctement le système vCenter Server et ses hôtes ESXi, selon le niveau d'intégration qui vous intéresse.

Niveau d'intégration	Privilèges requis
Collecte d'événements, de tâches et d'alarmes	<ul style="list-style-type: none"> ■ Système.Vue <p>Remarque Vue.Système est un privilège défini par le système. Lorsque vous ajoutez un rôle personnalisé et ne lui affectez pas de privilèges, le rôle est créé en tant que rôle en lecture seule avec trois privilèges définis par le système : Système.anonyme, Vue.système et Lecture.système.</p>
Configuration de Syslog sur les hôtes ESXi	<ul style="list-style-type: none"> ■ Hôte.Configuration.Modifier les paramètres ■ Hôte.Configuration.Configuration du réseau ■ Hôte.Configuration.Paramètres avancés ■ Hôte.Configuration.Profil de sécurité et pare-feu

Remarque Vous devez configurer l'autorisation dans le dossier de niveau supérieur de l'inventaire vCenter Server et vérifier que la case **Propager vers les enfants** est sélectionnée.

- Vérifiez que vous connaissez l'adresse IP ou le nom de domaine du système vCenter Server.
- Verify that you are logged in to the vRealize Log Insight *portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Sous Intégration, cliquez sur **vSphere**.
- 3 Tapez l'adresse IP et les informations d'identification d'une instance de vCenter Server, puis cliquez sur **Tester la connexion**.

Il est recommandé d'utiliser les informations d'identification du compte de service.

- 4 (Facultatif) Pour inscrire une autre instance de vCenter Server, cliquez sur **Ajouter vCenter Server** et répétez les étapes 3 à 5.

Remarque N'inscrivez pas des systèmes vCenter Server avec des noms ou des adresses IP en double. vRealize Log Insight ne recherche pas les noms d'instances de vCenter Server en double. Vous devez vérifier que la liste des systèmes vCenter Server inscrits ne contient aucune entrée en double.

- 5 Click **Save**.

Suivant

- Commencez à collecter les données d'événements, de tâches et d'alarmes de l'instance de vCenter Server que vous avez inscrite. Reportez-vous à [Configurer vRealize Log Insight pour l'extraction des événements, des tâches et des alarmes d'une instance de vCenter Server](#).
- Commencez à collecter les flux Syslog des hôtes ESXi gérés par l'instance de vCenter Server. Reportez-vous à [Configurer un hôte ESXi pour le transfert des événements de journaux à vRealize Log Insight](#).

vRealize Log Insight en tant que serveur Syslog

vRealize Log Insight inclut un serveur syslog intégré qui est constamment actif lorsque le service de vRealize Log Insight est en cours d'exécution.

Le serveur syslog écoute sur les ports 514/TCP, 1514/TCP et 514/UDP et est prêt à ajouter les messages de journaux qui sont envoyés à partir d'autres hôtes. Les messages qui sont ingérés par le serveur syslog peuvent faire l'objet d'une recherche dans l'interface utilisateur Web de vRealize Log Insight en temps quasi réel. La longueur maximale de message syslog acceptée par vRealize Log Insight est de 10 Ko.

Configurer un hôte ESXi pour le transfert des événements de journaux à vRealize Log Insight

Les hôtes ESXi ou les instances vCenter Server Appliance génèrent des données de journaux non structurées qui peuvent être analysées dans vRealize Log Insight.

Utilisez l'interface d'administration de vRealize Log Insight pour configurer les hôtes ESXi sur une instance de vCenter Server inscrite afin que les données Syslog soient envoyées vers vRealize Log Insight.

Avertissement L'exécution de tâches de configuration en parallèle peut entraîner des erreurs de paramètres Syslog sur les hôtes ESXi cibles. Assurez-vous qu'aucun autre utilisateur Admin n'est en train de configurer les mêmes hôtes ESXi que vous prévoyez de configurer.

Un cluster vRealize Log Insight peut distribuer les flux Syslog d'ESXi et de vCenter Server Appliance entre ses nœuds individuels à l'aide d'un équilibrage de charge.

Pour obtenir des informations sur le filtrage des messages syslog sur des hôtes ESXi avant l'envoi des messages à vRealize Log Insight, reportez-vous à la rubrique *Configurer le filtrage de journaux sur les hôtes ESXi* dans la section [Configuration d'ESXi](#) du guide **Installation et configuration de vSphere**.

Pour plus d'informations sur la configuration des flux Syslog à partir d'un vCenter Server Appliance, reportez-vous à [Configurer vCenter Server pour le transfert des événements de journaux à vRealize Log Insight](#).


Remarque vRealize Log Insight peut recevoir des données Syslog des hôtes ESXi versions 5.5 et ultérieures.

Prérequis

- Vérifiez que l'instance de vCenter Server qui gère l'hôte ESXi est inscrite auprès de votre instance de vRealize Log Insight. Ou bien vous pouvez enregistrer l'hôte ESXi et configurer vCenter Server en une seule opération.
- Vérifiez que vos informations d'identification d'utilisateur disposent des privilèges suffisants pour configurer Syslog sur les hôtes ESXi.
 - **Hôte.Configuration.Paramètres avancés**
 - **Hôte.Configuration.Profil de sécurité et pare-feu**

Remarque Vous devez configurer l'autorisation dans le dossier de niveau supérieur de l'inventaire vCenter Server et vérifier que la case **Propager vers les enfants** est sélectionnée.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Sous Intégration, cliquez sur **vSphere**.
- 3 Localisez l'instance de vCenter Server qui gère l'hôte ESXi dont vous souhaitez recevoir les flux Syslog.
- 4 Cochez la case **Configurer des hôtes ESXi pour l'envoi de journaux à Log Insight**.
 Par défaut, vRealize Log Insight configure tous les hôtes ESXi accessibles exécutant la version 5.5 ou des versions ultérieures de manière à ce qu'ils envoient leurs journaux via UDP.
- 5 (Facultatif) Pour modifier les valeurs de configuration par défaut, cliquez sur **Options avancées**.
 - Pour modifier le protocole pour tous les hôtes ESXi, sélectionnez **Configurer tous les hôtes ESXi**, sélectionnez un protocole, puis cliquez sur **OK**.
 - Pour ne configurer que la journalisation d'hôtes ESX spécifiques ou pour modifier le protocole des hôtes ESXi sélectionnés, suivez les étapes ci-dessous :
 - a Sélectionnez **Configurer des hôtes ESXi spécifiques**.
 - b Sélectionnez un ou plusieurs hôtes dans la liste **Filtrer par hôte**.
 - c Définissez la valeur de protocole.
 - d Cliquez sur **OK**.
- 6 (Facultatif) Si vous utilisez des clusters, ouvrez le menu déroulant de la zone de texte **Cible**, puis sélectionnez le nom d'hôte ou l'adresse IP de l'équilibrage de charge qui distribue les flux Syslog.
- 7 Click **Save**.

Modifier une configuration d'hôte ESXi pour le transfert des événements de journaux à vRealize Log Insight

Les hôtes ESXi ou les instances vCenter Server Appliance génèrent des données de journaux non structurées qui peuvent être analysées dans vRealize Log Insight.

Utilisez l'interface d'administration de vRealize Log Insight pour configurer les hôtes ESXi sur une instance de vCenter Server inscrite afin que les données Syslog soient envoyées vers vRealize Log Insight.

Avertissement L'exécution de tâches de configuration en parallèle peut entraîner des erreurs de paramètres Syslog sur les hôtes ESXi cibles. Assurez-vous qu'aucun autre utilisateur Admin n'est en train de configurer les mêmes hôtes ESXi que vous prévoyez de configurer.

Lorsque la configuration initiale est terminée, vous pouvez activer une option pour configurer automatiquement un hôte ESXi avec le protocole par défaut lorsqu'il est ajouté à un cluster.

Un cluster vRealize Log Insight peut distribuer les flux Syslog d'ESXi et de vCenter Server Appliance entre ses nœuds individuels à l'aide d'un équilibrage de charge.

Pour plus d'informations sur le filtrage des messages Syslog sur des hôtes ESXi avant l'envoi de messages configurés à vRealize Log Insight, reportez-vous à la rubrique *Configurer le filtrage de journaux sur les hôtes ESXi* dans la section [Configuration d'ESXi](#) du guide **Installation et configuration de vSphere**.

Pour plus d'informations sur la configuration des flux Syslog à partir d'un vCenter Server Appliance, reportez-vous à [Configurer vCenter Server pour le transfert des événements de journaux à vRealize Log Insight](#).

Remarque vRealize Log Insight peut recevoir des données Syslog des hôtes ESXi versions 5.5 et ultérieures.

Prérequis

- Vérifiez que l'instance de vCenter Server qui gère l'hôte ESXi est inscrite auprès de votre instance de vRealize Log Insight.
- Vérifiez que vos informations d'identification d'utilisateur disposent des privilèges suffisants pour configurer Syslog sur les hôtes ESXi.
 - **Hôte.Configuration.Paramètres avancés**
 - **Hôte.Configuration.Profil de sécurité et pare-feu**

Remarque Vous devez configurer l'autorisation dans le dossier de niveau supérieur de l'inventaire vCenter Server et vérifier que la case **Propager vers les enfants** est sélectionnée.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.

- 2 Sous Intégration, cliquez sur **vSphere**.
- 3 Cochez la case **Configurer des hôtes ESXi pour l'envoi de journaux à Log Insight**.
- 4 Cliquez sur **Options avancées**.
- 5 Pour modifier le protocole pour des hôtes ESXi sélectionnés, procédez comme suit :
 - a Sélectionnez un ou plusieurs hôtes dans la liste **Filtrer par hôte**.
 - b Définissez la valeur de protocole.
 - c Pour décider d'associer automatiquement le protocole par défaut à un hôte ESXi lorsqu'il est ajouté à un cluster vRealize Log Insight, sélectionnez **Configurer automatiquement tous les hôtes ESXi**.
 - d Cliquez sur **Configurer**.
- 6 (Facultatif) Si vous utilisez des clusters, vous pouvez spécifier un équilibrage de charge, ouvrir le menu déroulant de la zone de texte **Cible** sur l'écran **Intégration de vSphere** et sélectionner le nom d'hôte ou l'adresse IP de l'équilibrage de charge.

Événements de notification vRealize Log Insight dans vRealize Operations Manager

Vous pouvez configurer vRealize Log Insight de manière à envoyer des événements de notification à vRealize Operations Manager à partir des requêtes d'alertes que vous créez.

Lorsque vous configurez une alerte de notification dans vRealize Log Insight, vous sélectionnez dans vRealize Operations Manager une ressource associée aux événements de notification. Reportez-vous à [Ajouter une requête d'alerte à Log Insight pour l'envoi d'événements de notification à vRealize Operations Manager](#).

Les sections de l'interface utilisateur de vRealize Operations Manager où les événements de notification apparaissent sont répertoriées ci-dessous.

- Page d'accueil > tableau de bord **Recommandations** > widget **Principales alertes de santé concernant les descendants**
- Page d'accueil > onglet **Alertes**
- Sur tous les tableaux de bord personnalisés comprenant des widgets avec événements de notification

Pour obtenir des informations supplémentaires sur l'emplacement où les événements de notification apparaissent, reportez-vous au [Centre de documentation de VMware vRealize Operations Manager](#).

Configurer vCenter Server pour le transfert des événements de journaux à vRealize Log Insight

L'intégration vSphere collecte des tâches et événements de vCenter Server, mais pas les journaux internes de niveau faible de chaque composant vCenter Server. Ces journaux sont exploités par le pack de contenu vSphere.

La configuration de vCenter Server 6.5 et versions ultérieures doit être effectuée via l'interface de gestion de vCenter Server Appliance. Pour plus d'informations sur le transfert d'événements de journal à partir de vCenter Server, consultez la documentation de vSphere sur la redirection des fichiers journaux de vCenter Server Appliance vers une autre machine.

Pour les versions antérieures de vSphere, bien que vCenter Server Appliance contienne un démon Syslog qui pourrait être utilisé pour acheminer les journaux, la méthode privilégiée consiste à installer un agent vRealize Log Insight.

Pour obtenir des informations sur l'installation d'agents vRealize Log Insight, reportez-vous au *vRealize Log Insight Guide d'administration de l'agent* dans le centre d'informations [vRealize Log Insight](#).

Le pack de contenu vSphere contient des groupes d'agents qui définissent des fichiers journaux spécifiques à collecter depuis les installations de vCenter Server. La configuration est visible à l'adresse suivante : `https://LogInsightServerFqdnOrIP/contentpack?contentPackId=com.vmware.vsphere`.

Pour obtenir des informations sur l'utilisation des groupes d'agents, reportez-vous à [Chapitre 9 Utilisation des groupes d'agents](#)

Pour obtenir des informations sur les emplacements des fichiers journaux vCenter Server, reportez-vous à <http://kb.vmware.com/kb/1021804> et à <http://kb.vmware.com/kb/1021806>.

Configurer vRealize Log Insight pour l'extraction des événements, des tâches et des alarmes d'une instance de vCenter Server

Les événements, les tâches et les alertes sont des données structurées qui ont une signification particulière. Vous pouvez configurer vRealize Log Insight de manière à collecter les alarmes, les événements et les tâches d'un ou de plusieurs systèmes vCenter Server.

Vous devez utiliser l'interface utilisateur d'administration pour configurer vRealize Log Insight pour la connexion aux systèmes vCenter Server. Les informations sont extraites des systèmes vCenter Server à l'aide de vSphere Web Services API. Elles s'affichent sous forme de module de contenu vSphere dans l'interface utilisateur Web de vRealize Log Insight.


Remarque vRealize Log Insight ne peut extraire les alarmes, événements et tâches qu'à partir des instances de vCenter Server vCenter Server 5.1 et version ultérieure.

Prérequis

Vérifiez que vos informations d'identification disposent des privilèges **System.View**.

Remarque Vous devez configurer l'autorisation dans le dossier de niveau supérieur de l'inventaire vCenter Server et vérifier que la case **Propager vers les enfants** est sélectionnée.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Sous Intégration, cliquez sur **vSphere**.
- 3 Localisez l'instance de vCenter Server dont vous souhaitez collecter les données, puis cochez la case **Collecter les événements, les tâches et les alarmes de vCenter Server**.
- 4 Click **Save**.

vRealize Log Insight se connecte à l'instance de vCenter Server toutes les deux minutes et ingère toutes les informations apparues depuis la dernière interrogation.

Suivant

- Analysez les événements vSphere à l'aide du module de contenu vSphere ou des requêtes personnalisées.
- Activez les alertes du module de contenu vSphere ou les alertes personnalisées.

Utilisation de vRealize Operations Manager avec vRealize Log Insight

Conditions requises pour l'intégration à vRealize Operations Manager

Pour intégrer vRealize Log Insight à vRealize Operations Manager, vous devez indiquer les informations d'identification de vRealize Log Insight afin d'être authentifié auprès de vRealize Operations Manager. vRealize Operations Manager prend en charge les comptes d'utilisateurs locaux ainsi que plusieurs sources LDAP.

Pour déterminer le nom d'utilisateur d'un compte d'utilisateur local :

- 1 Ouvrez l'interface Web de vRealize Operations Manager.
- 2 Sélectionnez **Contrôle d'accès**.
- 3 Identifiez ou créez l'utilisateur d'intégration. Le champ Type de source est **Utilisateur local**.
- 4 Le nom d'utilisateur qui doit être saisi dans l'interface utilisateur d'administration de vRealize Log Insight est le contenu du champ **Nom d'utilisateur**.

Pour déterminer le format du nom d'utilisateur du compte d'utilisateur LDAP à fournir à vRealize Log Insight, suivez les instructions ci-dessous :

- 1 Ouvrez l'interface Web de vRealize Operations Manager.
- 2 Sélectionnez Contrôle d'accès.
- 3 Identifiez ou créez l'utilisateur d'intégration. Notez les champs **Nom d'utilisateur** et **Type de source**. Par exemple, un utilisateur nommé **integration@example.com** issu de la source **Active Directory - ad**.
- 4 Sélectionnez **Sources d'authentification**.
- 5 Identifiez la source d'authentification correspondant au **Type de source** de l'étape 3. Notez le champ **Nom complet de la source**. Par exemple, « ad ».
- 6 Le nom d'utilisateur qui doit être saisi dans l'interface utilisateur d'administration de vRealize Log Insight, sous la forme `UserName@SourceDisplayName`, est une combinaison de l'étape 3 et de l'étape 5. Par exemple, `integration@example.com@ad`.

Prérequis

Assurez-vous que le compte d'utilisateur d'intégration dispose des autorisations pour manipuler les objets dans vRealize Operations Manager. Reportez-vous à [Autorisations minimales requises pour un compte d'utilisateur local ou Active Directory](#).

Autorisations minimales requises pour un compte d'utilisateur local ou Active Directory

Pour intégrer vRealize Log Insight à vRealize Operations Manager, vous devez indiquer les informations d'identification de vRealize Log Insight afin d'être authentifié auprès de vRealize Operations Manager.

Pour manipuler des objets dans vRealize Operations Manager, un compte d'utilisateur doit disposer des autorisations requises.

Licence de vRealize Operations Manager

Si vous attribuez des autorisations à un utilisateur pour le lancement contextuel, l'utilisateur peut également configurer l'intégration des alertes. Utilisez les informations dans le tableau de l'intégration des alertes pour attribuer des autorisations pour l'intégration des alertes uniquement.

Tableau 12-1. Intégration des alertes

Action	Autorisations et objets à sélectionner
Créez un rôle personnalisé avec les autorisations répertoriées.	<ol style="list-style-type: none"> Administration -> Gestion des types de ressources [Vérifier tout] Administration -> Gestion des ressources [Vérifier tout] Administration -> API Rest <ol style="list-style-type: none"> Toutes les autres API de lecture et d'écriture Accès en lecture aux API
Attribuez le rôle précédent à l'utilisateur local ou Active Directory (nouveau ou existant) et sélectionnez des objets/hierarchies d'objet à attribuer.	<ol style="list-style-type: none"> Instance de l'adaptateur -> vRealizeOpsMgrAPI [Vérifier tout] Hôtes et clusters vSphere [Vérifier tout] Mise en réseau vSphere [Vérifier tout] Stockage vSphere [Vérifier tout]

Pour que l'intégration du lancement contextuel fonctionne, il faut un utilisateur disposant de privilèges d'administrateur. Si les alertes et le lancement contextuel sont activés, un utilisateur ayant des privilèges d'administrateur est requis.

Action	Autorisations et objets à sélectionner
Attribuez le rôle Administrateur à un compte d'utilisateur.	<p>Dans l'onglet Objets sur la page Attribuer des groupes et des autorisations :</p> <ol style="list-style-type: none"> Pour Sélectionner un rôle, sélectionnez Administrateur. Sélectionnez Attribuer ce rôle à l'utilisateur. Sélectionnez Autoriser l'accès à tous les objets du système.

Configurer vRealize Log Insight pour envoyer des événements de notification à vRealize Operations Manager

Vous pouvez configurer vRealize Log Insight pour envoyer des notifications d'alerte à vRealize Operations Manager.

Vous pouvez intégrer vRealize Log Insight au vApp vRealize Operations Manager et à la version installable de vRealize Operations Manager. Pour l'intégrer à la version installable, vous devez apporter des modifications supplémentaires à la configuration de vRealize Operations Manager. Pour plus d'informations sur la configuration de la version installable de vRealize Operations Manager dans le but de l'intégrer à vRealize Log Insight, reportez-vous au *Guide de démarrage de Log Insight*.

L'intégration des alertes vRealize Log Insight à vRealize Operations Manager permet d'afficher toutes les informations relatives à votre environnement dans une interface utilisateur unique.

Vous pouvez envoyer des événements de notification à partir de plusieurs instances de vRealize Log Insight vers une instance de vRealize Operations Manager unique. Vous pouvez activer le lancement contextuel pour une instance de vRealize Log Insight unique par instance de vRealize Operations Manager.


vRealize Log Insight utilise REST API de vRealize Operations Manager pour créer des ressources et des relations dans vRealize Operations Manager afin de configurer l'adaptateur de lancement contextuel.

Prérequis

- Créez un compte d'utilisateur d'intégration dans vRealize Operations Manager avec les autorisations requises. Pour plus d'informations, consultez [Conditions requises pour l'intégration à vRealize Operations Manager](#).
- Vérifiez que vous connaissez l'adresse IP ou le nom de domaine de l'instance de vRealize Operations Manager cible.
- Verify that you are logged in to the vRealize Log Insight *portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Remarque Dans un environnement exécutant un cluster vRealize Operations Manager avec un équilibrage de charge configuré, vous pouvez utiliser l'adresse IP de l'équilibrage de charge, le cas échéant.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Integration, select **vRealize Operations Manager**.
- 3 Tapez l'adresse IP ou le nom d'hôte du nœud maître de l'équilibrage de charge, s'il est configuré. Utilisez les informations d'identification de l'utilisateur de vRealize Operations Manager et cliquez sur **Tester la connexion**. vRealize Log Insight utilise les informations d'identification pour transmettre les événements de notification à vRealize Operations Manager. Assurez-vous que l'utilisateur configuré dispose des autorisations minimales requises pour garantir le bon fonctionnement de l'intégration. Reportez-vous à [Autorisations minimales requises pour un compte d'utilisateur local ou Active Directory](#).
- 4 Dans le volet vRealize Operations Manager, sélectionnez **Activer l'intégration des alertes**.
- 5 Click **Save**.

Suivant

- Consultez les pages correspondantes dans l'interface utilisateur de vRealize Operations Manager pour voir les événements de notification envoyés par vRealize Log Insight.

Activer le lancement contextuel de vRealize Log Insight dans vRealize Operations Manager

Vous pouvez configurer vRealize Operations Manager de manière à afficher des éléments de menu relatifs à vRealize Log Insight et à lancer vRealize Log Insight avec une requête spécifique à l'objet.

Vous pouvez intégrer vRealize Log Insight au vApp vRealize Operations Manager et à la version installable de vRealize Operations Manager.

L'intégration au vApp et à la version installable (Windows, Linux) nécessite d'apporter d'autres modifications à la configuration de vRealize Operations Manager. Reportez-vous à la rubrique relative à l'installation de vRealize Log Insight Management Pack (adaptateur) dans vRealize Operations Manager 6.x et versions ultérieures, dans le centre d'informations de [vRealize Log Insight 4.0](#).

Notez que vRealize Log Insight Management Pack est préinstallé dans vRealize Operations Manager 6.0 et versions ultérieures et qu'aucune modification de configuration n'est requise.


La version installable de vRealize Operations Manager (version Windows) n'est plus disponible pour vRealize Operations Manager 6.5 et versions ultérieures.

Important Une instance de vRealize Operations Manager ne prend en charge le lancement contextuel que pour une seule instance de vRealize Log Insight. vRealize Log Insight ne vérifie pas si d'autres instances sont déjà inscrites auprès de vRealize Operations Manager ; vous pouvez donc être amené à remplacer les paramètres d'un autre utilisateur.

Prérequis

- Verify that you are logged in to the vRealize Log Insight *portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.
- Vérifiez que vous connaissez l'adresse IP ou le nom de domaine de l'instance de vRealize Operations Manager cible.
- Vérifiez que vous disposez des informations d'identification utilisateur requises. Reportez-vous à [Autorisations minimales requises pour un compte d'utilisateur local ou Active Directory](#).
- Si vous utilisez vRealize Operations Manager 6.5 ou une version ultérieure, utilisez la procédure pour activer le lancement contextuel dans le centre d'informations de [vRealize Operations Manager 6.5](#).

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Integration, select **vRealize Operations Manager**.
- 3 Tapez l'adresse IP ou le nom de domaine complet du nœud maître ou de l'équilibrage de charge de vRealize Operations Manager, le cas échéant, et cliquez sur **Tester la connexion**.

Remarque Pour la fonctionnalité Lancement contextuel, vous devez indiquer un utilisateur de vRealize Operations Manager disposant des privilèges d'administrateur.

- 4 Click **Save**.

vRealize Log Insight configure l'instance de vRealize Operations Manager. Cette opération peut prendre quelques minutes.

Des éléments relatifs à vRealize Log Insight apparaissent dans les menus de vRealize Operations Manager.

Suivant

Lancez une requête vRealize Log Insight depuis l'instance de vRealize Operations Manager. Reportez-vous à [Lancement contextuel de vRealize Log Insight](#)

Lancement contextuel de vRealize Log Insight

Lorsque vous activez le lancement contextuel pour vRealize Log Insight, une ressource vRealize Log Insight est créée dans vRealize Operations Manager.

L'identificateur de la ressource contient l'adresse IP de l'instance de vRealize Log Insight ; il est utilisé par vRealize Operations Manager pour ouvrir vRealize Log Insight.

Lancement contextuel dans vRealize Operations Manager 6.5 et versions ultérieures

Pour plus d'informations sur l'activation du lancement contextuel, reportez-vous au centre d'informations de [vRealize Operations Manager](#).

Lancement contextuel dans l'interface utilisateur vSphere de vRealize Operations Manager 6.4 et versions antérieures

Les options de lancement contextuel relatives à vRealize Log Insight s'affichent dans le menu déroulant **Actions** de l'interface utilisateur vSphere. Ces éléments de menu vous permettent d'ouvrir vRealize Log Insight et de rechercher des événements de journaux à partir d'un objet de vRealize Operations Manager.

L'action de lancement contextuel disponible dépend de l'objet sélectionné dans l'inventaire vRealize Operations Manager. L'intervalle de temps des requêtes est limité à 60 minutes avant l'activation d'une option de lancement contextuel.

Tableau 12-3. Objets de l'interface utilisateur de vRealize Operations Manager et leurs options et actions de lancement contextuel

Objet sélectionné dans vRealize Operations Manager	Option de lancement contextuel dans le menu déroulant Actions	Action dans vRealize Operations Manager	Action dans vRealize Log Insight
Monde	Ouvrir vRealize Log Insight	Ouvre vRealize Log Insight.	vRealize Log Insight affiche l'onglet Analyse interactive .
vCenter Server	Ouvrir vRealize Log Insight	Ouvre vRealize Log Insight.	vRealize Log Insight affiche l'onglet Analyse interactive .
Centre de données	Rechercher des journaux dans vRealize Log Insight	Ouvre vRealize Log Insight et transfère le nom des ressources de tous les systèmes hôtes en dessous de l'objet de centre de données sélectionné.	vRealize Log Insight affiche l'onglet Analyse interactive et lance une requête afin de rechercher les événements de journaux contenant des noms d'hôtes dans le centre de données.

Tableau 12-3. Objets de l'interface utilisateur de vRealize Operations Manager et leurs options et actions de lancement contextuel (suite)


Objet sélectionné dans vRealize Operations Manager	Option de lancement contextuel dans le menu déroulant Actions	Action dans vRealize Operations Manager	Action dans vRealize Log Insight
Cluster	Rechercher des journaux dans vRealize Log Insight	Ouvre vRealize Log Insight et transfère le nom des ressources de tous les systèmes hôtes en dessous de l'objet de cluster sélectionné.	vRealize Log Insight affiche l'onglet Analyse interactive et lance une requête afin de rechercher les événements de journaux contenant des noms d'hôtes dans le cluster.
Système hôte	Rechercher des journaux dans vRealize Log Insight	Ouvre vRealize Log Insight et transfère le nom de la ressource de l'objet d'hôte sélectionné.	vRealize Log Insight affiche l'onglet Analyse interactive et lance une requête afin de rechercher les événements de journaux contenant le nom du système hôte sélectionné.
Machine virtuelle	Rechercher des journaux dans vRealize Log Insight	Ouvre vRealize Log Insight et transfère l'adresse IP de la machine virtuelle sélectionnée et le nom de la ressource du système hôte associé.	vRealize Log Insight affiche l'onglet Analyse interactive et lance une requête afin de rechercher les événements de journaux contenant l'adresse IP de la machine virtuelle et le nom de l'hôte où réside la machine virtuelle.

Si, dans l'onglet **Alertes**, vous sélectionnez une alerte et choisissez **Rechercher des journaux dans Log Insight** dans le menu contextuel, l'intervalle de temps de la requête est limité à une heure avant le déclenchement de l'alerte. Cela signifie que si une alerte a été déclenchée à 14 h 00, par exemple, la requête dans vRealize Log Insight affiche tous les messages de journaux se produisant entre 13 h 00 et 14 h 00. Cela vous aide à identifier les événements ayant pu déclencher l'alerte.

Vous pouvez ouvrir vRealize Log Insight depuis le diagramme de mesures de vRealize Operations Manager. L'intervalle de temps de la requête exécutée par vRealize Log Insight correspond à celle du diagramme de mesures.

Remarque L'heure du diagramme de mesures de vRealize Log Insight et celle du diagramme de mesures de vRealize Operations Manager peuvent varier si le paramètre d'heure des dispositifs virtuels est configuré différemment.

Lancement contextuel dans l'interface utilisateur de vRealize Operations Manager 6.4 et versions antérieures

L'icône de lancement contextuel  apparaît sur plusieurs pages de l'interface utilisateur, mais vous pouvez lancer vRealize Log Insight uniquement depuis les pages qui affichent des événements de notification de vRealize Log Insight :

- Page Présentation des alertes.

- La page Résumé de l'alerte d'une alerte de notification vRealize Log Insight.
- Les widgets Alertes de vos tableaux de bord, lorsqu'une alerte de notification vRealize Log Insight est sélectionnée.

Lorsque vous sélectionnez un événement de notification vRealize Log Insight dans l'interface utilisateur personnalisée, vous avez le choix entre deux actions de lancement contextuel.

Tableau 12-4. Options et actions de lancement contextuel dans l'interface utilisateur de vRealize Operations Manager

Option de lancement contextuel dans vRealize Operations Manager	Action dans vRealize Operations Manager	Action dans vRealize Log Insight
Ouvrir vRealize Log Insight	Ouvre vRealize Log Insight.	vRealize Log Insight affiche l'onglet Tableaux de bord et charge le tableau de bord de présentation de vSphere.
Rechercher des journaux dans vRealize Log Insight	Ouvre vRealize Log Insight et transfère l'ID de la requête qui a déclenché l'événement de notification.	vRealize Log Insight affiche l'onglet Analyse interactive et lance la requête qui a déclenché l'événement de notification.

Lorsque vous sélectionnez une alerte qui ne provient pas de vRealize Log Insight, l'élément **Rechercher les journaux de machines virtuelles et d'hôtes dans vRealize Log Insight** apparaît dans le menu de lancement contextuel. Si vous le sélectionnez, vRealize Operations Manager ouvre vRealize Log Insight et transfère les identifiants de l'objet ayant déclenché l'alerte. vRealize Log Insight lance une recherche dans les événements de journaux disponibles à l'aide des identifiants des ressources.

Lancement contextuel bilatéral

Le lancement contextuel est également accessible depuis vRealize Log Insight vers vRealize Operations Manager.

Si vous intégrez vRealize Log Insight à vRealize Operations Manager, vous pouvez exécuter un lancement contextuel à partir d'un événement vRealize Log Insight, en sélectionnant l'icône d'engrenage à gauche de l'événement et en sélectionnant l'option à afficher dans vRealize Operations Manager.

Pour plus d'informations sur le lancement contextuel depuis vRealize Operations Manager vers vRealize Log Insight, reportez-vous à la section [Lancement contextuel de vRealize Log Insight](#).

Procédure

- 1 Dans vRealize Log Insight, accédez à l'onglet **Analyse interactive**.
- 2 Localisez un événement qui contient des champs de mappage d'inventaire et placez le pointeur de la souris sur l'événement.

- 3 Cliquez sur l'icône d'engrenage et sélectionnez **Ouvrir analyse** dans vRealize Operations Manager via le menu déroulant.

Un nouvel onglet de navigateur s'ouvre et vous dirige vers l'instance de vRealize Operations Manager intégrée à vRealize Log Insight. Une fois authentifié, vous êtes dirigé vers la section **Environnement > Analyse** de vRealize Operations Manager avec l'objet sélectionné.

Remarque Si plusieurs instances de vRealize Log Insight sont connectées à la même instance de vRealize Operations Manager, seule la dernière instance de vRealize Log Insight intégrée à vRealize Operations Manager dispose de la fonctionnalité de lancement contextuel. Cela signifie également que la fonctionnalité de lancement contextuel est remplacée dès qu'une instance de vRealize Log Insight est intégrée à une instance de vRealize Operations Manager qui était intégrée précédemment à une autre instance de vRealize Log Insight.

Désactiver le lancement contextuel de vRealize Log Insight dans vRealize Operations Manager

Pour supprimer les éléments de menu relatifs à vRealize Log Insight dans l'interface utilisateur de vRealize Operations Manager, désinstallez l'adaptateur vRealize Log Insight de l'instance de vRealize Operations Manager.


Utilisez l'interface utilisateur d'administration de vRealize Log Insight pour désactiver le lancement contextuel. Si vous n'avez pas accès à vRealize Log Insight ou si l'instance de vRealize Log Insight est supprimée avant la désactivation de la connexion à vRealize Operations Manager, vous pouvez annuler l'inscription de vRealize Log Insight dans l'interface utilisateur d'administration de vRealize Operations Manager. Pour ce faire, reportez-vous à l'aide dans le portail d'administration de vRealize Operations Manager.

Avertissement Une instance de vRealize Operations Manager ne prend en charge le lancement contextuel que pour une seule instance de vRealize Log Insight. Si une autre instance de vRealize Log Insight a été inscrite après l'inscription de l'instance à désactiver, la dernière instance écrase les paramètres de la précédente sans vous avertir.

Prérequis

- Verify that you are logged in to the vRealize Log Insight *portnumber* Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procédure

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Integration, select **vRealize Operations Manager**.
- 3 Décochez la case **Activer le lancement contextuel**.
- 4 Click **Save**.

vRealize Log Insight configure l'instance de vRealize Operations Manager de manière à supprimer l'adaptateur de vRealize Log Insight. Cette opération peut prendre quelques minutes.

Ajouter un chemin et un domaine de recherche DNS

Vous pouvez ajouter un chemin et un domaine de recherche DNS pour améliorer la correspondance d'inventaire de vRealize Operations Manager.

L'ajout d'un chemin et d'un domaine de recherche DNS améliore la correspondance lorsque l'intitulé d'une machine virtuelle et un domaine de recherche sont résolus en adresse IP de l'hôte qui envoie des messages de journaux à vRealize Log Insight. Par exemple, si vous disposez d'une machine virtuelle nommée `linux_01` dans vRealize Operations Manager et si le nom d'hôte `linux_01.company.com` est résolu en `192.168.10.10`, l'ajout d'un domaine de recherche permet à vRealize Log Insight de reconnaître et de correspondre à cette ressource.

Procédure

- 1 Effectuez un arrêt de l'invité du dispositif virtuel vRealize Log Insight.
- 2 Une fois la machine virtuelle sous tension, sélectionnez **Modifier les paramètres**.
- 3 Sélectionnez l'onglet **Options**.
- 4 Dans **Options vApp > Avancé**, cliquez sur **Propriétés**.
- 5 Recherchez les clés `vami.searchpath.VMware_vCenter_Log_Insight` et `vami.domain.VMware_vCenter_Log_Insight`.
Si les valeurs n'existent pas, créez-les.
- 6 Définissez le chemin et le domaine de recherche DNS.
- 7 Mettez le dispositif virtuel sous tension.

Suivant

Lorsque vRealize Log Insight démarre, vous pouvez valider la configuration DNS en vous connectant et en affichant le contenu du fichier `/etc/resolv.conf` file. Les options de recherche et de domaine doivent apparaître dans le bas du fichier.

Supprimer l'adaptateur vRealize Log Insight

Lorsque vous activez le lancement contextuel sur une instance de vRealize Operations Manager 6.2 et versions ultérieures, vRealize Log Insight crée une instance de l'adaptateur vRealize Log Insight sur l'instance de vRealize Operations Manager.

L'instance de l'adaptateur reste sur l'instance de vRealize Operations Manager lorsque vous désinstallez vRealize Log Insight. Par conséquent, les éléments de menu du lancement contextuel continuent à apparaître dans les menus d'actions et pointent vers une instance de vRealize Log Insight qui n'existe plus.

Pour désactiver la fonctionnalité de lancement contextuel dans vRealize Operations Manager, vous devez supprimer l'adaptateur vRealize Log Insight de l'instance de vRealize Operations Manager.

Vous pouvez envoyer des appels REST à vRealize Operations Manager à l'aide de l'utilitaire de ligne de commande cURL.

Remarque Ces mesures ne sont nécessaires que si le lancement contextuel a été activé.

Prérequis

- Vérifiez que cURL est installé sur votre système. Notez que cet outil est préinstallé dans le dispositif virtuel vRealize Operations Manager et que les étapes peuvent être réalisées à partir du dispositif à l'aide de l'adresse IP 127.0.0.1.
- Vérifiez que vous connaissez l'adresse IP ou le nom de domaine de l'instance de vRealize Operations Manager cible.
- En fonction de la licence de vRealize Operations Manager que vous possédez, vérifiez que vous disposez des informations d'identification minimales requises pour supprimer le module de gestion. Reportez-vous à [Autorisations minimales requises pour un compte d'utilisateur local ou Active Directory](#).

Procédure

- 1 Dans cURL, recherchez l'adaptateur vRealize Log Insight en exécutant la requête suivante dans le dispositif virtuel vRealize Operations Manager.

```
curl -k -u "admin" https://ipaddress/suite-api/api/adapterkinds/LogInsight/resourcekinds/LogInsightLogServer/resources
```

Où *admin* est le nom de connexion de l'administrateur et *ipaddress* est l'adresse IP (ou le nom d'hôte) de l'instance de vRealize Operations Manager. Vous êtes invité à entrer le mot de passe de l'utilisateur : *admin*.

Dans la sortie cURL, recherchez la valeur du GUID attribuée à l'identificateur : `<ops:resource creationTime="{TIMESTAMP}" identifier="{GUID}">`. Vous pouvez utiliser cette valeur de GUID dans la commande ci-dessous qui permet de supprimer l'instance d'adaptateur.

- 2 Supprimez l'adaptateur vRealize Log Insight en exécutant la commande suivante.

```
curl -k -u "admin" -X DELETE https://ipaddress/suite-api/api/adapters/{GUID}
```

Où *admin* est le nom de connexion de l'administrateur et *ipaddress* est l'adresse IP (ou le nom d'hôte) de l'instance de vRealize Operations Manager. Vous êtes invité à entrer le mot de passe de l'utilisateur : *admin*.

Les éléments relatifs au lancement contextuel de vRealize Log Insight sont supprimés des menus de vRealize Operations Manager. Pour plus d'informations sur le lancement contextuel, reportez-vous à la rubrique *Lancement contextuel de vRealize Log Insight*, dans l'aide de vRealize Log Insight.

Pack de contenu de vRealize Operations Manager pour vRealize Log Insight

Le pack de contenu de vRealize Operations Manager pour vRealize Log Insight contient des tableaux de bord, des champs extraits, des requêtes enregistrées et des alertes qui s'utilisent pour analyser tous les journaux redirigés depuis une instance de vRealize Operations Manager.

Le pack de contenu de vRealize Operations Manager vous permet d'analyser tous les journaux redirigés depuis une instance de vRealize Operations Manager. Il contient des tableaux de bord, des requêtes et des alertes grâce auxquels l'administrateur de vRealize Operations Manager peut réaliser des actions de dépannage et de diagnostic. Pour faciliter leur gestion, les tableaux de bord sont groupés en fonction des composants principaux de vRealize Operations Manager, tels qu'Analyse, Interface utilisateur et Adaptateurs. Vous pouvez activer différentes alertes pour l'envoi d'e-mails et d'événements de notification de vRealize Operations Manager aux administrateurs.

Vous pouvez télécharger le pack de contenu de vRealize Operations Manager à l'adresse https://solutionexchange.vmware.com/store/loginsight?src=Product_Product_LogInsight_YES_US.

Reportez-vous à [Utilisation des packs de contenu](#).

Considérations en matière de sécurité de vRealize Log Insight

13

Utilisez les fonctionnalités de vRealize Log Insight pour sécuriser votre environnement contre les attaques.

Ce chapitre aborde les rubriques suivantes :

- [Ports et interfaces externes](#)
- [Fichiers de configuration de vRealize Log Insight](#)
- [Clé publique, certificat et keystore de vRealize Log Insight](#)
- [Fichier de licence et CLUF de vRealize Log Insight](#)
- [Fichiers journaux de vRealize Log Insight](#)
- [Comptes d'utilisateurs vRealize Log Insight](#)
- [Recommandations relatives au pare-feu pour vRealize Log Insight](#)
- [Correctifs et mises à jour de sécurité](#)

Ports et interfaces externes

vRealize Log Insight utilise des services, des ports et des interfaces externes spécifiques requis.

Ports de communication

vRealize Log Insight utilise les ports et les protocoles de communication énumérés dans cette rubrique. Les ports requis sont organisés selon qu'ils sont requis pour les sources, pour l'interface utilisateur, entre des clusters, pour les services externes, ou selon qu'ils peuvent être bloqués en toute sécurité par un pare-feu. Certains ports sont utilisés uniquement si vous activez l'intégration correspondante.

Remarque vRealize Log Insight ne prend pas en charge le clustering WAN (également appelé géoclustering, clustering haute disponibilité ou clustering distant). Tous les nœuds du cluster doivent être déployés dans le même réseau local de couche 2. En outre, les ports décrits dans cette section doivent être ouverts entre les nœuds pour garantir une bonne communication.

Le trafic réseau de vRealize Log Insight dispose de plusieurs sources.

Poste de travail administrateur	Machine utilisée par un administrateur système pour gérer le dispositif virtuel vRealize Log Insight à distance.
Poste de travail utilisateur	Machine sur laquelle un utilisateur vRealize Log Insight accède à l'interface Web de vRealize Log Insight à l'aide d'un navigateur.
Système envoyant des journaux	Point de terminaison qui envoie des journaux à vRealize Log Insight pour effectuer une analyse et une recherche. Les points de terminaison sont par exemple des hôtes ESXi, des machines virtuelles ou tout système doté d'une adresse IP.
Log Insight Agents	Agent qui réside sur une machine Windows ou Linux et envoie des journaux et des événements du système d'exploitation à vRealize Log Insight par des API.
Dispositif vRealize Log Insight	Tout dispositif virtuel vRealize Log Insight (maître ou travailleur) sur lequel résident les services vRealize Log Insight. Le système d'exploitation de base du dispositif est SUSE 11 SP3.

Ports requis pour les sources envoyant des données

Les ports suivants doivent être ouverts pour le trafic réseau depuis des sources qui envoient des données à vRealize Log Insight, pour les connexions depuis l'extérieur du cluster et pour les connexions équilibrées en charge entre les nœuds de cluster.

Source	Destination	Port	Protocole	Description du service
Système envoyant des journaux	Dispositif vRealize Log Insight	514	TCP, UDP	Trafic syslog sortant configuré en tant que destination de redirecteur
Système envoyant des journaux	Dispositif vRealize Log Insight	1514, 6514	TCP	Données Syslog via SSL
Agents vRealize Log Insight	Dispositif vRealize Log Insight	9000	TCP	API Ingestion de Log Insight
Agents vRealize Log Insight	Dispositif vRealize Log Insight	9543	TCP	API Ingestion de Log Insight par SSL

Ports requis pour l'interface utilisateur

Les ports suivants doivent être ouverts pour le trafic réseau qui doit utiliser l'interface utilisateur vRealize Log Insight, pour les connexions à l'extérieur du cluster et pour les connexions équilibrées en charge entre les nœuds de cluster.

Source	Destination	Port	Protocole	Description du service
Poste de travail administrateur	Dispositif vRealize Log Insight	22	TCP	SSH : connectivité Secure Shell
Poste de travail utilisateur	Dispositif vRealize Log Insight	80	TCP	HTTP : interface Web
Poste de travail utilisateur	Dispositif vRealize Log Insight	443	TCP	HTTPS : interface Web

Ports requis entre des nœuds de clusters

Les ports suivant doivent uniquement être ouverts sur un nœud maître vRealize Log Insight pour un accès réseau depuis des nœuds travailleurs, pour une sécurité optimale. Ces ports s'ajoutent aux ports utilisés pour les sources et le trafic d'interface utilisateur qui sont équilibrés en charge entre les nœuds de cluster.

Source	Destination	Port	Protocole	Description du service
Dispositif vRealize Log Insight	Dispositif vRealize Log Insight	7000	TCP	Requête et réplication Cassandra
Dispositif vRealize Log Insight	Dispositif vRealize Log Insight	9042	TCP	Service Cassandra pour les clients de protocole natif
Dispositif vRealize Log Insight	Dispositif vRealize Log Insight	9160	TCP	Service Cassandra pour les clients Thrift
Dispositif vRealize Log Insight	Dispositif vRealize Log Insight	59778, 16520-16580	TCP	Service vRealize Log Insight Thrift

Ports requis pour les services externes

Les ports suivants doivent être ouverts pour le trafic de réseau sortant depuis des nœuds de cluster de vRealize Log Insight vers des services distants.

Source	Destination	Port	Protocole	Description du service
Dispositif vRealize Log Insight	serveur NTP	123	UDP	NTPD : permet la synchronisation de l'heure NTP
				Remarque Le port est ouvert uniquement si vous décidez d'utiliser la synchronisation de l'heure NTP
Dispositif vRealize Log Insight	Serveur de messagerie	25	TCP	SMTP : service de messagerie pour alertes sortantes

Source	Destination	Port	Protocole	Description du service
Dispositif vRealize Log Insight	Serveur de messagerie	465	TCP	SMTPS : service de messagerie via SSL pour alertes sortantes
Dispositif vRealize Log Insight	Serveur DNS	53	TCP, UDP	DNS : service de résolution de noms
Dispositif vRealize Log Insight	Serveur AD	389	TCP, UDP	Active Directory
Dispositif vRealize Log Insight	Serveur AD	636	TCP	Active Directory via SSL
Dispositif vRealize Log Insight	Serveur AD	3268	TCP	Catalogue global Active Directory
Dispositif vRealize Log Insight	Serveur AD	3269	TCP	Protocole SSL de catalogue global Active Directory
Dispositif vRealize Log Insight	Serveur AD	88	TCP, UDP	Kerberos
Dispositif vRealize Log Insight	vCenter Server	443	TCP	Service Web vCenter Server
Dispositif vRealize Log Insight	Dispositif vRealize Operations Manager	443	TCP	Service Web vRealize Operations
Dispositif vRealize Log Insight	Gestionnaire de journaux tiers	514	TCP, UDP	Données Syslog
Dispositif vRealize Log Insight	Gestionnaire de journaux tiers	9000	CFAPI	Trafic d'API Log Insight Ingestion (CFAPI) sortant configuré en tant que destination de redirecteur
Dispositif vRealize Log Insight	Gestionnaire de journaux tiers	9543	CFAPI	Trafic d'API Log Insight Ingestion (CFAPI) sortant configuré en tant que destination de redirecteur avec chiffrement (SSL/TLS)

Ports pouvant être bloqués

Les ports suivants sont ouverts, mais ne sont pas utilisés par vRealize Log Insight. Ces ports peuvent être bloqués en toute sécurité par un pare-feu.

Destination	Port	Protocole	Description du service
Dispositif vRealize Log Insight	111	TCP, UDP	Service RPCbind qui convertit les numéros du programme RPC en adresses universelles
Service Tomcat de dispositif vRealize Log Insight	9007	TCP	Services Tomcat

Fichiers de configuration de vRealize Log Insight

Les paramètres de certains fichiers de configuration ont une incidence sur la sécurité dans vRealize Log Insight.

Remarque Toutes les ressources liées à la sécurité sont accessibles depuis le compte racine. La protection de ce compte est indispensable à la sécurité de vRealize Log Insight.

Tableau 13-1. Fichiers de configuration de Log Insight

Fichier	Description
/usr/lib/loginsight/application/etc/loginsight-config-base.xml	Configuration du système par défaut pour vRealize Log Insight.
/storage/core/loginsight/config/loginsight-config.xml#number	Configuration du système modifiée (par rapport la configuration par défaut) pour vRealize Log Insight.
/usr/lib/loginsight/application/etc/jaas.conf	Configuration pour l'intégration d'Active Directory.
/usr/lib/loginsight/application/etc/3rd_config/server.xml	Configuration du système pour le serveur Apache Tomcat.
/storage/var/loginsight/apache-tomcat/conf/tomcat-users.xml	Configuration du système pour le serveur Apache Tomcat.
/usr/lib/loginsight/application/3rd_party/apache-tomcat-*/conf/server.xml	Configuration du système pour le serveur Apache Tomcat.
/usr/lib/loginsight/application/3rd_party/apache-tomcat-*/conf/tomcat-users.xml	Informations utilisateur pour le serveur Apache Tomcat.

Clé publique, certificat et keystore de vRealize Log Insight

La clé publique, le certificat et le keystore de vRealize Log Insight se trouvent sur le dispositif virtuel vRealize Log Insight.

Remarque Toutes les ressources liées à la sécurité sont accessibles depuis le compte racine. La protection de ce compte est indispensable à la sécurité de vRealize Log Insight.

- /usr/lib/loginsight/application/etc/public.cert
- /usr/lib/loginsight/application/etc/loginsight.pub
- /usr/lib/loginsight/application/etc/3rd_config/keystore

- `/usr/lib/loginsight/application/etc/truststore`
- `/usr/lib/loginsight/application/3rd_party/apache-tomcat-*/conf/keystore`

Fichier de licence et CLUF de vRealize Log Insight

Le Contrat de Licence Utilisateur Final (CLUF) et le fichier de licence se trouvent sur le dispositif virtuel vRealize Log Insight.

Remarque Toutes les ressources liées à la sécurité sont accessibles depuis le compte racine. La protection de ce compte est indispensable à la sécurité de vRealize Log Insight.

Fichier	Emplacement
Licence	<code>/usr/lib/loginsight/application/etc/license/loginsight_dev.dlf</code>
Licence	<code>/usr/lib/loginsight/application/etc/license/loginsight_cpu.dlf</code>
Licence	<code>/usr/lib/loginsight/application/etc/license/loginsight_osi.dlf</code>
Fichier de clé de licence	<code>/usr/lib/loginsight/application/etc/license/loginsight_license.bak</code>
Contrat de Licence Utilisateur Final	<code>/usr/lib/loginsight/application/etc/license/release/eula.txt</code>

Fichiers journaux de vRealize Log Insight

Les fichiers contenant les messages système se trouvent sur le dispositif virtuel vRealize Log Insight.

Fichier	Description
<code>/storage/var/loginsight/alert.log</code>	Utilisé pour suivre les informations sur les alertes définies par l'utilisateur ayant été déclenchées.
<code>/storage/var/loginsight/apache-tomcat/logs/*.log</code>	Utilisé pour suivre les événements du serveur Apache Tomcat.
<code>/storage/var/loginsight/cassandra.log</code>	Utilisé pour suivre le stockage et la réplication de la configuration du cluster dans Apache Cassandra.
<code>/storage/var/loginsight/plugins/vsphere/li-vsphere.log</code>	Utilisé pour suivre les événements associés à l'intégration avec vSphere Web Client.
<code>/storage/var/loginsight/loginsight_daemon_stdout.log</code>	Utilisé pour la sortie standard du démon vRealize Log Insight.
<code>/storage/var/loginsight/phonehome.log</code>	Utilisé pour suivre les informations sur la collecte des données de trace envoyées à VMware (si l'option est activée).
<code>/storage/var/loginsight/pi.log</code>	Utilisé pour suivre les événements de début ou de fin de la base de données.
<code>/storage/var/loginsight/runtime.log</code>	Utilisé pour suivre l'ensemble des informations relatives au temps d'exécution associées à vRealize Log Insight.
<code>/var/log/firstboot/stratavm.log</code>	Utilisé pour suivre les événements ayant lieu au premier démarrage et à la première configuration du dispositif virtuel vRealize Log Insight.

Fichier	Description
/storage/var/loginsight/systemalert.log	Utilisé pour suivre les informations sur les notifications système envoyées par vRealize Log Insight. Chaque alerte est répertoriée en tant qu'entrée JSON.
/storage/var/loginsight/systemalert_worker.log	Utilisé pour suivre les informations sur les notifications système envoyées par un nœud travailleur de vRealize Log Insight. Chaque alerte est répertoriée en tant qu'entrée JSON.
/storage/var/loginsight/ui.log	Utilisé pour suivre les événements associés à l'interface utilisateur de vRealize Log Insight.
/storage/var/loginsight/ui_runtime.log	Utilisé pour suivre les événements d'exécution associés à l'interface utilisateur de vRealize Log Insight.
/storage/var/loginsight/upgrade.log	Utilisé pour suivre les événements ayant lieu pendant la mise à niveau de vRealize Log Insight.
/storage/var/loginsight/usage.log	Utilisé pour suivre toutes les requêtes.
/storage/var/loginsight/vcenter_operations.log	Utilisé pour suivre les événements associés à l'intégration de vRealize Operations Manager.
/storage/var/loginsight/watchdog_log*	Utilisé pour suivre les événements de temps d'exécution du processus de surveillance, responsable du redémarrage de vRealize Log Insight en cas d'arrêt.

Messages de journaux relatifs à la sécurité

Le fichier `ui_runtime.log` contient des messages de journaux d'audit d'utilisateur au format suivant.

- [2013-05-17 20:40:18.716+0000] [http-443-5 INFO /127.0.0.1]
[com.vmware.loginsight.web.actions.misc.LoginActionBean][User logged in: Name: admin | Role: admin]
- [2013-05-17 20:39:51.395+0000] [http-443-5 INFO /127.0.0.1]
[com.vmware.loginsight.web.actions.misc.LoginActionBean][User logged out: Name: admin | Role: admin]
- [2013-09-18 12:39:34.823-0700] [http-9443-3 WARN /127.0.0.1]
[com.vmware.loginsight.web.actions.misc.LoginActionBean][Bad username/password attempt (username: myusername)]
- [2013-09-18 12:40:08.761-0700] [http-9443-3 INFO /127.0.0.1]
[com.vmware.loginsight.web.actions.misc.LoginActionBean][User logged in: Active Directory User: SAM=myusername, Domain=vmware.com,UPN=myusername@vmware.com]
- [2013-09-18 12:40:20.232-0700] [http-9443-3 INFO /127.0.0.1]
[com.vmware.loginsight.web.actions.misc.LoginActionBean][User logged in: Active Directory User: SAM=myusername, Domain=vmware.com,UPN=myusername@vmware.com]
- [2013-09-18 12:40:36.933-0700] [http-9443-3 INFO /127.0.0.1]
[com.vmware.loginsight.web.actions.misc.LoginActionBean][User logged in: Local User: Name=myusername, Role=user]

- [2013-09-18 12:40:40.429-0700] [http-9443-3 INFO /127.0.0.1]
[com.vmware.loginsight.web.actions.misc.LoginActionBean] [User logged out: Local User: Name=myusername, Role=user]
- [2013-11-13 23:26:21.569+0000] [http-443-4 INFO /127.0.0.1]
[com.vmware.loginsight.web.actions.settings.UsersActionBean] [Created new user: Active Directory User: SAM=username, Domain=vmware.com, UPN=username@vmware.com]
- [2013-11-14 22:44:11.017+0000] [http-443-6 INFO /127.0.0.1]
[com.vmware.loginsight.web.actions.settings.UsersActionBean] [Created new user: Local User: Name=username, Role=admin]
- [2013-12-05 21:03:36.751+0000] [http-443-3 INFO /127.0.0.1]
[com.vmware.loginsight.web.actions.settings.UsersActionBean] [Removed users: Active Directory User: SAM=username, Domain=vmware.com, UPN=username@vmware.com]]
- [2013-12-05 21:04:16.707+0000] [http-443-3 INFO /127.0.0.1]
[com.vmware.loginsight.web.actions.settings.UsersActionBean] [Removed users: Local User: Name=username, Role=admin]]
- [http-9443-3 INFO /127.0.0.1]
[com.vmware.loginsight.web.actions.settings.UsersActionBean] [Created new group: (domain=vmware.com, group=VMware Employees, role=user)]
- [2013-12-05 13:07:04.108-0800] [http-9443-2 INFO /127.0.0.1]
[com.vmware.loginsight.web.actions.settings.UsersActionBean] [Removed groups: [(domain=vmware.com, group=VMware Employees, role=user)]]

Comptes d'utilisateurs vRealize Log Insight

Pour administrer vRealize Log Insight, vous devez définir un compte système et un compte racine.

Utilisateur racine de vRealize Log Insight

vRealize Log Insight utilise actuellement le compte d'utilisateur racine en tant qu'utilisateur du service. Aucun autre utilisateur n'est créé.

Le mot de passe racine par défaut est vide, sauf si vous avez défini la propriété du mot de passe racine lors du déploiement. Vous devez modifier ce mot de passe lors de la première connexion à la console de vRealize Log Insight.

SSH est désactivé tant que le mot de passe racine n'a pas été défini.

Le mot de passe racine doit répondre aux critères suivants.

- Il doit contenir au moins 8 caractères.
- Il doit contenir au moins une majuscule, une minuscule, un chiffre et un caractère spécial.
- Le même caractère ne doit pas être répété plus de trois fois.

Utilisateur Admin de vRealize Log Insight

Lorsque vous démarrez le dispositif virtuel vRealize Log Insight pour la première fois, vRealize Log Insight crée le compte d'utilisateur Admin pour son interface utilisateur Web.

Le mot de passe pour l'utilisateur Admin est vide par défaut. Vous devez modifier ce mot de passe dans l'interface utilisateur Web lors de la configuration initiale de vRealize Log Insight.

Prise en charge d'Active Directory

vRealize Log Insight prend en charge l'intégration avec Active Directory. Une fois cette option configurée, vRealize Log Insight peut authentifier ou autoriser un utilisateur à travers Active Directory.

Reportez-vous à [Permettre l'authentification utilisateur à travers Active Directory](#).

Privilèges attribués aux utilisateurs par défaut

L'utilisateur du service vRealize Log Insight dispose de privilèges racine.

L'utilisateur Admin de l'interface utilisateur Web dispose des privilèges d'administrateur uniquement sur l'interface utilisateur Web de vRealize Log Insight.

Recommandations relatives au pare-feu pour vRealize Log Insight

Pour protéger les informations sensibles rassemblées par vRealize Log Insight, placez le ou les serveurs sur un segment de réseau de gestion protégé du reste de votre réseau interne par un pare-feu.

Ports requis

Les ports suivants doivent être ouverts au trafic réseau sur les sources qui envoient des données à vRealize Log Insight.

Port	Protocole
514/UDP, 514/TCP	Syslog
1514/TCP, 6514/TCP	Syslog-TLS (SSL)
9000/TCP	API Ingestion de vRealize Log Insight
9543/TCP	API Ingestion de vRealize Log Insight - TLS (SSL)

Les ports suivants doivent être ouverts au trafic réseau qui utilise l'interface utilisateur de vRealize Log Insight.

Port	Protocole
80/TCP	HTTP
443/TCP	HTTPS

L'ensemble de ports suivant doit uniquement être ouvert sur un nœud maître vRealize Log Insight pour un accès réseau depuis des nœuds travailleurs, pour une sécurité optimale.

Port	Protocole
16520:16580/TCP	RPC Thrift
59778/TCP	Serveur log4j
12543/TCP	Serveur de base de données

Correctifs et mises à jour de sécurité

Le dispositif virtuel vRealize Log Insight utilise SUSE Linux Enterprise Server 11 (x86_64) version 11 et niveau de correctif 3 en tant que système d'exploitation invité.

VMware publiera des correctifs pour résoudre les problèmes de sécurité.

Avant d'appliquer une mise à niveau ou un correctif au système d'exploitation invité, tenez compte des dépendances. Reportez-vous à [Chapitre 6 Ports et interfaces externes](#).

Sauvegarde, restauration et récupération d'urgence

14

Pour éviter les dépenses liées aux temps d'arrêt des centres de données, suivez ces meilleures pratiques d'exécution d'opérations de sauvegarde, restauration et récupération d'urgence vRealize Log Insight.

Ce chapitre aborde les rubriques suivantes :

- [Présentation des opérations de sauvegarde, restauration et récupération d'urgence](#)
- [Utilisation d'adresses IP statiques et de noms de domaines complets](#)
- [Planification et préparation](#)
- [Sauvegarder des nœuds et des clusters](#)
- [Agents de sauvegarde Linux ou Windows](#)
- [Restaurer des nœuds et des clusters](#)
- [Modification de configurations après restauration](#)
- [Vérifier les restaurations](#)
- [Récupération d'urgence](#)

Présentation des opérations de sauvegarde, restauration et récupération d'urgence

VMware fournit un portefeuille intégré complet de solutions de BCDR (Continuité d'activité et de récupération d'urgence) qui offrent haute disponibilité, protection des données et récupération d'urgence.

Utilisez les informations sur la sauvegarde, la restauration et la récupération d'urgence contenues dans ce document pour les composants de vRealize Log Insight, notamment le nœud master, le nœud worker et le redirecteur.

- Pour plus d'informations sur les membres des clusters master et worker, notamment la configuration, les données des journaux et la personnalisation, consultez [Sauvegarder des nœuds et des clusters](#).
- Pour plus d'informations sur la configuration locale d'agent Linux ou Windows, consultez [Agents de sauvegarde Linux ou Windows](#).

Les informations contenues dans ce document ne s'appliquent pas aux outils et produits suivants. Vous devez rechercher des informations sur ces outils et produits dans différentes ressources.

- Outils tiers spécifiquement utilisés pour la sauvegarde, la restauration et la récupération d'urgence. Pour plus d'informations, consultez la documentation du fournisseur.

- vSphere Data Protection, Site Recovery Manager et Symantec NetBackup. Pour plus d'informations sur les solutions de continuité d'activité et de récupération d'urgence de VMware, reportez-vous à <http://www.vmware.com/business-continuity/business-continuity> et à la [documentation VMware vCloud Suite](#).
- Capacité de sauvegarde, de restauration et de récupération d'urgence pour les produits intégrés à vRealize Log Insight.
 - vRealize Operations Manager
 - Serveur vSphere Web Client
 - Hôtes ESXi

Utilisation d'adresses IP statiques et de noms de domaines complets

Vous pouvez utiliser des adresses IP statiques et des noms de domaines complets pour éviter tout problème au cours des opérations de sauvegarde, restauration et récupération d'urgence.

Adresses IP statiques pour nœuds de cluster et équilibrage de charge vRealize Log Insight

Si vous utilisez des adresses IP statiques pour tous les nœuds d'un cluster vRealize Log Insight, cela vous évite d'avoir à mettre à jour les adresses IP des nœuds du cluster lorsqu'elles sont modifiées.

vRealize Log Insight inclut toutes les adresses IP de nœuds dans chaque fichier de configuration des nœuds de cluster comme décrit dans [l'article 2123058 de la base de connaissances](#)

Tous les produits intégrés à vRealize Log Insight (ESXi, vSphere, vRealize Operations) utilisent le nom de domaine complet ou l'adresse IP du nœud maître du cluster comme cible Syslog. Ces produits peuvent utiliser le nom de domaine complet ou l'adresse IP de l'équilibrage de charge, s'il est configuré, comme cible Syslog. Les adresses IP statiques réduisent le risque lié au fait de constamment mettre à jour l'adresse IP de la cible Syslog à plusieurs emplacements.

Indiquez des adresses IP statiques et des adresses IP virtuelles facultatives pour l'équilibrage de charge. Lorsque vous configurez un équilibrage de charge intégré, indiquez le nom de domaine complet facultatif comme adresse IP virtuelle. Le nom de domaine complet est utilisé si l'adresse IP n'est pas accessible pour une raison quelconque.

Nom de domaine complet pour nœuds de cluster et nœud travailleur vRealize Log Insight

Lorsque vous utilisez un nom de domaine complet pour tous les nœuds du cluster vRealize Log Insight, vous évitez les modifications de configuration de récupération et d'après restauration, en supposant que le nom de domaine puisse être résolu sur le site de récupération.

Pour le nœud maître (équilibrage de charge s'il est utilisé), un nom de domaine complet pouvant être entièrement résolu est requis. Sinon, les hôtes ESXi ne peuvent pas transmettre les messages Syslog à vRealize Log Insight ou à toute cible distante.

Pour les notifications système, vRealize Log Insight utilise des noms d'hôtes de noms de domaine complets s'ils sont disponibles à la place d'adresses IP.

Vous pouvez raisonnablement supposer que seules les adresses IP sous-jacentes sont modifiées après les opérations de sauvegarde, restauration et récupération d'urgence. L'utilisation du nom de domaine complet évite d'avoir à modifier l'adresse cible Syslog (nom de domaine complet du nœud maître ou de l'équilibrage de charge interne) sur tous les périphériques externes qui transmettent des journaux au cluster vRealize Log Insight.

Vérifiez que les demandes de jonction d'un nœud travailleur vRealize Log Insight utilisent le nom de domaine complet du nœud maître vRealize Log Insight.

La valeur hôte du nœud maître indiquée dans le fichier de configuration sur chacun des nœuds est basée sur la valeur utilisée par le premier nœud travailleur qui envoie une demande de jonction. L'utilisation du nom de domaine complet du nœud maître pour la demande de jonction permet d'éviter d'apporter des modifications manuelles à la valeur hôte du nœud maître après une récupération d'urgence. Sinon, les nœuds travailleurs ne peuvent pas rejoindre le nœud maître tant que le nom d'hôte du nœud maître n'est pas mis à jour dans les fichiers de configuration sur tous les nœuds de clusters restaurés.

Planification et préparation

Avant de mettre en œuvre une sauvegarde, une restauration ou une procédure de récupération d'urgence, consultez les informations de planification et de préparation dans cette rubrique.

Les recommandations suivantes doivent être prises en compte dans un plan de sauvegarde, de restauration et de récupération d'urgence.

Tester les opérations de sauvegarde

Effectuez un test des opérations de sauvegarde, restauration et récupération d'urgence dans un environnement de test ou intermédiaire avant de les exécuter dans une installation de production en direct.

Effectuez une sauvegarde complète de l'intégralité du cluster vRealize Log Insight. N'utilisez pas de procédures automatiques pour la sauvegarde des configurations et fichiers individuels.

Vérifier les correctifs

Vérifiez que les correctifs sont implémentés et que les avertissements et erreurs sont résolus avant d'effectuer des opérations de sauvegarde, restauration et récupération d'urgence. Les outils de sauvegarde, de restauration et de récupération d'urgence fournissent généralement des validations visuelles et des étapes permettant de vérifier la création des configurations de sauvegarde, restauration et récupération d'urgence.

Planification des sauvegardes

Selon la configuration du cluster, la première opération de sauvegarde est généralement une sauvegarde complète. Prévoyez un certain temps pour la première sauvegarde. Les sauvegardes suivantes, qu'il s'agisse de sauvegardes incrémentielles ou complètes, sont relativement plus rapides que la première opération de sauvegarde.

Documentation et outils supplémentaires

Assurez-vous de suivre la documentation relative à l'allocation des ressources pour les outils de sauvegarde, de restauration et de récupération d'urgence vRealize Log Insight.

Assurez-vous de suivre les meilleures pratiques et recommandations spécifiques des outils tiers de sauvegarde, restauration et récupération d'urgence.

Pour les machines virtuelles déployées avec des produits VMware, utilisez des outils supplémentaires contenant des fonctionnalités et des configurations spécifiques pour prendre en charge les opérations de sauvegarde, de restauration et de récupération d'urgence.

Redirecteurs et clusters

Pour les redirecteurs, appliquez les étapes de sauvegarde, restauration et récupération d'urgence du cluster vRealize Log Insight principal. Reportez-vous à [Restaurer des nœuds et des clusters](#).

Selon la configuration requise du client, vous pouvez utiliser un seul ou plusieurs redirecteurs vRealize Log Insight. En outre, les redirecteurs peuvent être installés en tant que nœud autonome ou en tant que cluster. Pour les opérations de sauvegarde, restauration et récupération d'urgence, les redirecteurs vRealize Log Insight sont identiques aux nœuds du cluster vRealize Log Insight principal et sont traités de la même manière.

Sauvegarder des nœuds et des clusters

Il est recommandé de configurer des sauvegardes ou une réplication planifiées des nœuds et des clusters vRealize Log Insight.

vRealize Log Insight ne prend pas en charge les snapshots suspendus. Si vous essayez de créer un snapshot suspendu, il est créé, mais la suspension n'est pas appliquée. Pour plus d'informations, consultez l'article de la base de connaissances de VMware [Log Insight virtual appliance becomes unresponsive during quiesced snapshots \(Un dispositif virtuel Log Insight ne répond plus lors de snapshots suspendus\)](#).

Prérequis

- Avant d'effectuer les opérations de sauvegarde ou de réplication, vérifiez qu'il n'existe pas de problèmes de configuration sur les sites source et cible.
- Vérifiez que l'allocation des ressources du cluster n'est pas au maximum de la capacité.

Dans les configurations contenant des charges raisonnables d'ingestion et de requête, l'utilisation de la mémoire et de l'échange peut atteindre près de 100 % de la capacité pendant les opérations de sauvegarde et de réplication. Comme la mémoire atteint près de 100 % de la capacité dans un environnement dynamique, le pic de mémoire est dû en partie à l'utilisation du cluster vRealize Log Insight. De plus, les opérations planifiées de sauvegarde et réplication peuvent contribuer de manière significative au pic de mémoire.

Dans certains cas, les nœuds travailleurs sont momentanément déconnectés pendant une à trois minutes avant de rejoindre les nœuds principaux en raison de l'utilisation élevée de la mémoire.

- Réduisez la limitation de mémoire sur les nœuds vRealize Log Insight en effectuant l'une des opérations suivantes ou les deux :
 - Allouez de la mémoire supplémentaire aux configurations recommandées de vRealize Log Insight.
 - Planifiez les sauvegardes récurrentes en dehors des heures de pointe.

Procédure

- 1 Activez la sauvegarde ou la réplication régulière des redirecteurs vRealize Log Insight en utilisant les mêmes procédures que celles du serveur vRealize Log Insight.
- 2 Vérifiez que la fréquence et les types de sauvegarde sont correctement sélectionnés en fonction des ressources disponibles et de la configuration requise spécifique du client.
- 3 Si les ressources ne posent pas de problème et si l'outil prend en charge ce type d'opération, activez les sauvegardes simultanées des nœuds du cluster pour accélérer le processus de sauvegarde.
- 4 Sauvegardez tous les nœuds en même temps.

Suivant

Surveillance : pendant la sauvegarde, vérifiez que la configuration de vRealize Log Insight ne présente pas de problèmes d'environnement ou de performance. La plupart des outils de sauvegarde, de restauration et de récupération d'urgence offrent des possibilités de surveillance.

Pendant le processus de sauvegarde, vérifiez tous les journaux pertinents sur le système de production, car il est possible que l'interface utilisateur n'affiche pas tous les problèmes.

Agents de sauvegarde Linux ou Windows

Vous sauvegardez des agents en sauvegardant des informations d'installation et de configuration sur le serveur. Il n'est pas nécessaire de sauvegarder séparément le nœud de l'agent.

En général, les agents sont installés sur des systèmes Linux ou Windows qui sont également utilisés pour d'autres applications ou services et ils peuvent être inclus dans des procédures de sauvegarde existantes. Une sauvegarde complète de niveau fichier ou de niveau bloc de la machine qui inclut l'intégralité de l'installation agent et sa configuration est suffisante pour la récupération. Les agents prennent en charge la configuration locale et la configuration fournie par le serveur.

Si l'agent est configuré intégralement depuis le serveur vRealize Log Insight, sans modification locale apportée au fichier de configuration `liagent.ini`, vous pouvez éviter de créer une sauvegarde de l'installation agent. Au lieu de cela, exécutez une nouvelle installation de l'agent et récupérez la sauvegarde du serveur.

Si l'agent dispose d'une configuration locale personnalisée, sauvegardez le fichier `liagent.ini` et restaurez-le avec une nouvelle installation de l'agent. Si vous utilisez les nœuds de l'agent au-delà de la simple installation du logiciel de l'agent et si ces nœuds nécessitent une sauvegarde complète, suivez la même procédure de sauvegarde que pour toute autre machine virtuelle.

Si la configuration de l'agent est effectuée côté client (sur les agents) et si les nœuds de l'agent servent uniquement à installer vRealize Log Insight le logiciel de l'agent, la sauvegarde du fichier de configuration de l'agent suffit.

Prérequis

Vérifiez que la configuration de l'agent se trouve sur vRealize Log Insight côté serveur.

Procédure

- 1 Sauvegardez le fichier `liagent.ini`.
- 2 Remplacez le fichier de l'agent récupéré ou de l'ordinateur Linux ou Windows par le fichier de sauvegarde.

Restaurer des nœuds et des clusters

Les nœuds doivent être restaurés dans un ordre spécifique et certains scénarios de restauration peuvent nécessiter des modifications de configuration manuelles.

Selon l'outil utilisé pour la restauration, vous pouvez restaurer les machines virtuelles sur le même hôte, sur un autre hôte du même centre de données ou sur un autre hôte d'un centre de données distant cible. Reportez-vous à [Modification de configurations après restauration](#)

Prérequis

- Vérifiez que les nœuds restaurés sont hors tension.
- Vérifiez que les instances du cluster sont hors tension avant de restaurer le cluster sur un nouveau site.
- Vérifiez qu'aucun syndrome Split-Brain ne se produit lorsque les mêmes adresses IP et les mêmes noms de domaine complets sont utilisés sur le site de récupération.
- Vérifiez qu'aucun utilisateur n'utilise accidentellement un cluster fonctionnant partiellement sur le site principal.

Procédure

- 1 Restaurez le nœud maître avant de restaurer les nœuds travailleurs.
- 2 Vous pouvez restaurer les nœuds travailleurs dans n'importe quel ordre.

3 (Facultatif) Restaurez les redirecteurs si vous les avez configurés.

Vérifiez que le serveur vRealize Log Insight (le nœud maître et tous les nœuds travailleurs dans une configuration de cluster) est restauré avant de restaurer les redirecteurs.

4 Restaurez les agents récupérés, le cas échéant.

Suivant

- Lors de la restauration d'un cluster vRealize Log Insight, si les mêmes adresses IP sont utilisées, vérifiez que les adresses IP et les noms de domaine complets de tous les nœuds restaurés sont associés à leurs contreparties initiales.

Le scénario suivant échouerait, par exemple : Dans un cluster composé des nœuds A, B et C, le nœud A est restauré avec l'adresse IP B, le nœud B avec l'adresse IP C et le nœud C avec l'adresse IP A.

- Si les mêmes adresses IP sont utilisées uniquement pour un sous-ensemble des nœuds restaurés, vérifiez pour ces nœuds que toutes les images restaurées sont associées à leur adresse IP d'origine.
- La plupart des outils de sauvegarde, de restauration et de récupération d'urgence contiennent une vue permettant de suivre la progression des opérations et d'identifier les pannes ou avertissements éventuels. Prenez les mesures appropriées pour résoudre le problème.
- Si des modifications de configuration manuelles sont requises avant la restauration complète du site, suivez les directives de la section [Modification de configurations après restauration](#).
- Une fois la restauration terminée, effectuez un contrôle partiel rapide du cluster qui a été restauré.

Modification de configurations après restauration

Les personnalisations de l'IP et de la cible de récupération lors de la configuration de la sauvegarde déterminent les configurations manuelles à modifier. Vous devez appliquer les modifications de configuration à un ou plusieurs nœuds vRealize Log Insight pour que le site restauré soit entièrement fonctionnel.

Restaurer sur le même hôte

La récupération d'un cluster vRealize Log Insight sur le même hôte est une opération simple qui peut être effectuée avec n'importe quel outil.

Prérequis

Consulter des informations importantes concernant [Planification et préparation](#).

Procédure

- 1 Mettez hors tension le cluster existant avant de lancer l'opération de restauration. Par défaut, les mêmes adresses IP et noms de domaine complets sont utilisés pour les nœuds de cluster restaurés.

- 2 (Facultatif) Indiquez un nouveau nom pour le cluster.

Pendant le processus de restauration, la copie d'origine du cluster est remplacée par la version restaurée, sauf si un nouveau nom est fourni à la machine virtuelle.

- 3 (Facultatif) Vérifiez si possible que tous les paramètres réseau, IP et nom de domaine complet utilisés pour l'environnement de production sont conservés sur le site restauré et récupéré.

Suivant

Une fois la restauration et le contrôle d'intégrité effectués, supprimez l'ancienne copie pour conserver les ressources et éviter un syndrome Split-Brain accidentel si un utilisateur met sous tension l'ancienne copie.

Restaurer sur un hôte différent

Lorsque vous effectuez une restauration sur un hôte différent, vous devez effectuer des modifications de configuration sur le cluster vRealize Log Insight.

Les modifications directes des fichiers de configuration à partir de la console du dispositif ne sont pas officiellement prises en charge dans vRealize Log Insight 3.0 et les versions ultérieures. Consultez [l'article 2123058 de la base de connaissances](#) pour plus d'informations sur la procédure à suivre pour apporter ces modifications à l'aide de l'interface utilisateur Web.

Ces modifications de configuration sont spécifiques aux builds vRealize Log Insight et peuvent être utilisées avec n'importe quel outil de récupération de sauvegarde.

La récupération sur un hôte différent nécessite des modifications de configuration manuelles sur le cluster vRealize Log Insight. Vous pouvez supposer que les nœuds vRealize Log Insight restaurés ont des adresses IP et des noms de domaine complets différents de ceux de leurs contreparties sources utilisées pour la sauvegarde.

Prérequis

Consulter des informations importantes concernant [Planification et préparation](#).

Procédure

- 1 Répertoriez toutes les nouvelles adresses IP et nouveaux noms de domaine complets qui ont été attribués à chaque nœud vRealize Log Insight.

2 Apportez les modifications de configuration suivantes sur le nœud maître en suivant la procédure décrite dans [l'article 2123058 de la base de connaissances](#).

- a Dans la section de configuration de vRealize Log Insight, recherchez les lignes qui sont semblables aux lignes suivantes.

```
<distributed overwrite-children="true">
  <daemon host="prod-es-vrli1.domain.com" port="16520" token="c4c4c6a7-f85c-4f28-
a48f-43aeea27cd0e">
    <service-group name="standalone" />
  </daemon>
  <daemon host="192.168.1.73" port="16520" token="a5c65b52-aff5-43ea-8a6d-38807ebc6167">
    <service-group name="workernode" />
  </daemon>
  <daemon host="192.168.1.74" port="16520" token="a2b57cb5-a6ac-48ee-8e10-17134e1e462e">
    <service-group name="workernode" />
  </daemon>
</distributed>
```

Le code affiche trois nœuds. Le premier est le nœud maître, qui affiche `<service-group name=standalone>`, et les deux autres sont des nœuds travailleurs, qui affichent `<service-group name="workernode">`

- b Pour le nœud maître, dans l'environnement récemment récupéré, vérifiez que l'entrée DNS utilisée dans l'environnement avant la récupération peut être réutilisée.
- Le cas échéant, mettez uniquement à jour l'entrée DNS pour qu'elle pointe vers la nouvelle adresse IP du nœud maître.
 - Si l'entrée DNS ne peut pas être réutilisée, remplacez l'entrée du nœud maître par un nouveau nom DNS (pointant vers la nouvelle adresse IP).
 - Si le nom DNS ne peut pas être attribué, comme dernière option, mettez à jour l'entrée de configuration avec la nouvelle adresse IP.
- c Mettez également à jour les adresses IP du nœud travailleur pour refléter les nouvelles adresses IP.

- d Dans le même fichier de configuration, vérifiez qu'il existe des entrées qui représentent les sections NTP, SMTP, database et appenders.

```
<ntp>
  <ntp-servers value="ntp1.domain.com, ntp2.domain.com" />
</ntp>

<smtp>
  <server value="smtp.domain.com" />
  <default-sender value="source.domain.com@domain.com" />
</smtp>

<database>
  <password value="xserttt" />
  <host value="vrli-node1.domain.com" />
  <port value="12543" />
</database>
```

- Si les valeurs de serveur NTP configurées ne sont plus valides dans le nouvel environnement, mettez-les à jour dans la section `<ntp>...</ntp>`.
 - Si les valeurs de serveur SMTP configurées ne sont plus valides dans le nouvel environnement, mettez-les à jour dans la section `<smtp>...</smtp>`.
 - Modifiez éventuellement la valeur `default-sender` dans la section SMTP. Vous pouvez utiliser n'importe quelle valeur, mais il est recommandé de représenter la source à partir de l'emplacement depuis lequel l'e-mail est envoyé.
 - Dans la section `<database>...</database>`, modifiez la valeur hôte pour pointer vers le nom de domaine complet ou l'adresse IP du nœud maître.
- e Dans le même fichier de configuration, mettez à jour la section de configuration de l'ILB vRealize Log Insight.

```
<load-balancer>
  <leadership-lease-renewal-secs value="5" />
  <high-availability-enabled value="true" />
  <high-availability-ip value="10.158.128.165" />
  <high-availability-fqdn value="LB-FQDN.eng.vmware.com" />
  <layer4-enabled value="true" />
  <ui-balancing-enabled value="true" />
</load-balancer>
```

- f Sous la section `<load-balancer>...</load-balancer>`, mettez à jour la valeur `high-availability-ip` si elle est différente du paramètre actuel.
- g Veillez également à mettre à jour le nom de domaine complet de l'équilibrage de charge.

- h Redémarrez l'interface utilisateur Web via l'onglet Cluster de la page Administration. Pour chaque nœud répertorié, sélectionnez son nom d'hôte ou son adresse IP pour ouvrir le panneau de détail, puis cliquez sur **Redémarrer Log Insight**.

Les modifications de configuration sont automatiquement appliquées à tous les nœuds de cluster.

- i Patientez deux minutes après le démarrage du service vRealize Log Insight pour permettre au service Cassandra de démarrer avant d'appeler d'autres nœuds travailleurs en ligne.

Suivant

Vérifiez que les nœuds vRealize Log Insight restaurés se sont vus attribuer des adresses IP et des noms de domaine complets différents de ceux attribués à leurs contreparties sources utilisées pour la sauvegarde.


Vérifier les restaurations

Vous devez vérifier que tous les clusters vRealize Log Insight restaurés sont entièrement fonctionnels.

Prérequis

Assurez-vous que le processus de sauvegarde et restauration est terminé avant de vérifier les configurations de nœud et de cluster.

Procédure

- 1 Connectez-vous à vRealize Log Insight à l'aide de l'adresse IP de l'équilibrage de charge interne (ILB) ou du nom de domaine complet (s'il est configuré).
- 2 Click the configuration drop-down menu icon  and select **Administration**.
- 3 Effectuez les vérifications suivantes :
 - a Vérifiez que vous pouvez accéder à tous les nœuds de cluster individuels via l'adresse IP ou le nom de domaine complet correspondant.
 - b Vérifiez l'état des nœuds du cluster sur la page Cluster et assurez-vous que l'ILB (s'il est configuré) est également dans un état actif.
 - c Vérifiez l'intégration de vSphere. Si nécessaire, reconfigurez l'intégration. Une reconfiguration s'impose lorsque l'adresse IP ou le nom de domaine complet du nœud maître et/ou de l'ILB est modifié après la récupération.
 - d Vérifiez l'intégration de vRealize Operations Manager et reconfigurez si nécessaire.
 - e Vérifiez que tous les packs de contenu et fonctionnalités de l'interface utilisateur fonctionnent correctement.
 - f Vérifiez que les redirecteurs et agents vRealize Log Insight fonctionnent correctement s'ils sont configurés.
- 4 Vérifiez que les autres fonctionnalités clés de vRealize Log Insight fonctionnent comme prévu.

Suivant

Si nécessaire, ajustez votre plan de sauvegarde et de récupération pour résoudre les éventuels problèmes identifiés au cours des opérations de sauvegarde, restauration et vérification.

Récupération d'urgence

Il est essentiel de disposer d'un plan de récupération bien documenté et testé pour renvoyer rapidement un cluster à son état de fonctionnement.

Le choix du type de réplication est déterminant lorsque vous configurez une machine virtuelle pour la récupération d'urgence. Pour ce faire, tenez compte de l'objectif de point de récupération (RPO), de l'objectif de temps de récupération (RTO), du coût et de l'évolutivité.

Dans un scénario de récupération d'urgence, il n'est pas toujours possible de restaurer le cluster sur le même site si le site principal est entièrement hors service. Selon l'option que vous choisissez, certaines étapes manuelles sont requises pour restaurer entièrement le cluster vRealize Log Insight et le renvoyer à son état de fonctionnement.

À moins que le cluster vRealize Log Insight ne soit entièrement hors service et inaccessible, assurez-vous que ses instances sont hors tension avant de le restaurer sur un nouveau site.

En cas de panne, récupérez le cluster vRealize Log Insight dès que possible.

Dépannage de vRealize Log Insight

15

Vous pouvez résoudre vous-même les problèmes courants relatifs à l'administration de vRealize Log Insight avant de contacter le support VMware.

Ce chapitre aborde les rubriques suivantes :

- [L'espace disque de vRealize Log Insight est épuisé](#)
- [L'importation de données archivées peut échouer](#)
- [Créer un bundle de support de vRealize Log Insight à l'aide de la console du dispositif virtuel](#)
- [Réinitialiser le mot de passe de l'utilisateur Admin](#)
- [Réinitialiser le mot de passe de l'utilisateur racine](#)
- [Des alertes n'ont pas pu être envoyées à vRealize Operations Manager](#)
- [Impossible de se connecter à l'aide des informations d'identification Active Directory](#)
- [SMTP ne fonctionne pas lorsque l'option STARTTLS est activée](#)
- [La mise à niveau échoue du fait que la signature du fichier .pak ne peut pas être validée](#)
- [La mise à niveau échoue en générant une erreur de serveur interne](#)

L'espace disque de vRealize Log Insight est épuisé

Si vous utilisez un disque virtuel de petite taille et que l'archivage n'est pas activé, l'espace disque d'un nœud maître ou travailleur vRealize Log Insight peut arriver à épuisement.

Problème

L'espace disque de vRealize Log Insight arrive à épuisement lorsque le débit d'entrée des journaux par minute est supérieur à 3 % de l'espace de stockage.

Cause

Dans une situation normale, l'espace disque de vRealize Log Insight ne s'épuise jamais, car le système vérifie toutes les minutes si l'espace disponible est inférieur à 3 %. Si l'espace disponible sur le dispositif virtuel vRealize Log Insight passe en dessous de 3 %, les compartiments de données anciens sont retirés.

Toutefois, si le disque est de petite taille et que le taux d'ingestion des journaux est élevé au point de remplir l'espace disque disponible (3 %) en moins d'une minute, l'espace disque de vRealize Log Insight arrive à épuisement.

Si l'archivage est activé, vRealize Log Insight archive le compartiment avant de le retirer. Si l'espace disponible est rempli avant l'archivage et le retrait du compartiment ancien, l'espace disque de vRealize Log Insight arrive à épuisement.

Solution

- ◆ Augmentez la capacité de stockage du dispositif virtuel vRealize Log Insight. Reportez-vous à [Augmenter la capacité de stockage du dispositif virtuel vRealize Log Insight](#).

L'importation de données archivées peut échouer

L'importation de données archivées peut échouer si le dispositif virtuel vRealize Log Insight ne dispose plus d'espace disque.

Problème

L'utilitaire d'importation de référentiel vRealize Log Insight ne recherche pas l'espace disque disponible sur le dispositif virtuel vRealize Log Insight. L'importation des fichiers journaux archivés peut donc échouer si le dispositif virtuel ne dispose plus d'espace disque.

Solution

Augmentez la capacité de stockage du dispositif virtuel vRealize Log Insight et redémarrez l'importation. [Augmenter la capacité de stockage du dispositif virtuel vRealize Log Insight](#). Toutefois, notez que les informations correctement importées avant l'échec seront dupliquées.

Créer un bundle de support de vRealize Log Insight à l'aide de la console du dispositif virtuel

Si vous ne pouvez pas accéder à l'interface utilisateur Web de vRealize Log Insight, vous pouvez télécharger le bundle de support à l'aide de la console du dispositif virtuel ou après avoir établi une connexion SSH avec le dispositif virtuel vRealize Log Insight.

Prérequis

- Verify that you have the root user credentials to log in to the vRealize Log Insight virtual appliance.
- If you plan to connect to the vRealize Log Insight virtual appliance by using SSH, verify that TCP port 22 is open.

Procédure

- 1 Établissez une connexion SSH au vApp vRealize Log Insight, puis connectez-vous en tant qu'utilisateur racine.

2 Pour générer le bundle de support, exécutez `loginsight-support`.

Pour générer un bundle de support et inclure uniquement les fichiers qui ont été modifiés au cours d'une période donnée, exécutez la commande `loginsight-support` avec la contrainte `--days`. Par exemple, `--days=1` inclut uniquement les fichiers modifiés depuis un jour.

Les données de support sont collectées et enregistrées dans un fichier `*.tar.gz` dont le nom est généré comme suit : `loginsight-support-YYYY-MM-DD_HHMMSS.xxxxx.tar.gz`, où `xxxxx` correspond à l'ID du processus d'exécution de `loginsight-support`.

Suivant

Transférez le bundle de support au support VMware, comme requis.

Réinitialiser le mot de passe de l'utilisateur Admin

Si un utilisateur Admin oublie le mot de passe de l'interface utilisateur Web, il ne peut plus accéder à son compte.

Problème

Si un seul utilisateur Admin a été défini pour vRealize Log Insight et que celui-ci oublie son mot de passe, l'application ne peut plus être administrée. Si l'utilisateur Admin est, de surcroît, le seul utilisateur défini pour vRealize Log Insight, l'ensemble de l'interface utilisateur Web devient inaccessible.

Cause

Un utilisateur Admin qui oublie son mot de passe ne dispose pas d'une interface utilisateur dans vRealize Log Insight qui lui permette de réinitialiser lui-même son mot de passe.

Remarque Les utilisateurs Admin qui sont en mesure de se connecter peuvent réinitialiser le mot de passe d'autres utilisateurs Admin. Réinitialisez le mot de passe de l'utilisateur Admin uniquement lorsque les mots de passe de tous les comptes d'utilisateurs Admin ont été oubliés.

Solution

Prérequis

- Vérifiez que vous disposez des informations d'identification de l'utilisateur racine pour vous connecter au dispositif virtuel vRealize Log Insight. Reportez-vous à [Configurer le mot de passe SSH racine du dispositif virtuel vRealize Log Insight](#)
- Pour activer les connexions SSH, vérifiez que le port TCP 22 est ouvert.

Procédure

- 1 Établissez une connexion SSH au dispositif virtuel vRealize Log Insight, puis connectez-vous en tant qu'utilisateur racine.

- 2 Tapez `li-reset-admin-passwd.sh` et appuyez sur **Entrée**.

Le script réinitialise le mot de passe de l'utilisateur Admin, en génère un nouveau et l'affiche à l'écran.

Suivant

Utilisez le nouveau mot de passe pour vous connecter à l'interface utilisateur Web de vRealize Log Insight, puis modifiez le mot de passe de l'utilisateur Admin.

Réinitialiser le mot de passe de l'utilisateur racine

Si vous oubliez le mot de passe de l'utilisateur racine, vous ne pouvez plus établir de connexion SSH ni utiliser la console du dispositif virtuel vRealize Log Insight.

Problème

Sans pouvoir établir de connexion SSH ni utiliser la console du dispositif virtuel vRealize Log Insight, vous ne pouvez pas réaliser certaines tâches administratives ni réinitialiser le mot de passe de l'utilisateur Admin.

Solution

Vous risquez de ne pas pouvoir vous connecter en tant que racine pour plusieurs raisons, notamment :

- Vous n'avez pas modifié le mot de passe par défaut. Par défaut, vRealize Log Insight définit un mot de passe vierge pour l'utilisateur racine et désactive l'accès SSH. Une fois le mot de passe défini, l'accès SSH pour l'utilisateur racine est activé.
- Vous pouvez définir une clé SSH lors du déploiement du dispositif virtuel vRealize Log Insight. Si une clé SSH est spécifiée via OVF, l'authentification par mot de passe est désactivée. Connectez-vous avec la clé SSH définie ou reportez-vous à la procédure décrite ci-dessous.
- Vous avez entré plusieurs fois un mot de passe incorrect et votre compte est momentanément verrouillé. Dans ce cas, la saisie du mot de passe correct ne vous permettra pas de vous connecter si la période de blocage n'est pas terminée. Patientez ou redémarrez le dispositif virtuel.

Procédure

- 1 Dans vSphere Client, exécutez un arrêt de l'invité du dispositif virtuel vRealize Log Insight.
- 2 Une fois la machine virtuelle hors tension, sélectionnez **Modifier les paramètres**.
- 3 Sélectionnez l'onglet **Options**.
- 4 Sous **Options vApp > Avancé**, sélectionnez **Propriétés**.
- 5 Recherchez et modifiez la clé `vm.rootpw`.

Si vous ne voyez pas la clé `vm.rootpw`, ajoutez une nouvelle clé.

Si vous utilisez des clés SSH au lieu de l'authentification par mot de passe, modifiez ou ajoutez la clé `vm.sshkey`.

6 Entrez un mot de passe.

Vous pouvez également ajouter une clé SSH ici si vous n'utilisez pas l'authentification par mot de passe.

7 Mettez le dispositif virtuel sous tension.

Suivant

Lorsque vRealize Log Insight démarre, confirmez que vous pouvez vous connecter en tant qu'utilisateur racine.

Des alertes n'ont pas pu être envoyées à vRealize Operations Manager

vRealize Log Insight vous informe en cas d'échec de l'envoi d'un événement d'alerte à vRealize Operations Manager. vRealize Log Insight retente d'envoyer l'alerte toutes les minutes, jusqu'à résolution du problème.

Problème

Un symbole rouge avec un point d'exclamation s'affiche sur la barre d'outils de vRealize Log Insight si une alerte n'a pas pu être envoyée à vRealize Operations Manager.

Cause

Des problèmes de connectivité empêchent vRealize Operations Manager vRealize Log Insight d'envoyer des notifications d'alerte à vRealize Operations Manager.

Solution

- Cliquez sur l'icône rouge pour ouvrir la liste des messages d'erreur, puis faites défiler cette dernière vers le bas pour consulter le dernier message.

Le symbole rouge sur la barre d'outils disparaît dès que vous ouvrez la liste des messages d'erreur ou si le problème est résolu.

- Pour résoudre le problème de connectivité avec vRealize Operations Manager, tentez ce qui suit.
 - Vérifiez que le vApp vRealize Operations Manager n'est pas arrêté.
 - Vérifiez que vous pouvez vous connecter à vRealize Operations Manager en utilisant le bouton **Tester la connexion** situé dans la section **vRealize Operations Manager** de la page **Administration** de l'interface utilisateur Web de vRealize Log Insight.
 - Vérifiez que vous disposez des informations d'identification correctes en vous connectant directement à vRealize Operations Manager.
 - Recherchez les éventuels messages concernant des problèmes de connectivité dans les journaux de vRealize Log Insight et de vRealize Operations Manager.
 - Vérifiez qu'aucune alerte n'a été éliminée dans l'interface utilisateur vSphere de vRealize Operations Manager.

Impossible de se connecter à l'aide des informations d'identification Active Directory

Vous ne pouvez pas vous connecter à l'interface utilisateur Web de vRealize Log Insight si vous utilisez les informations d'identification Active Directory.

Problème

Un administrateur a correctement ajouté votre compte Active Directory à vRealize Log Insight, mais vous ne pouvez pas vous connecter à vRealize Log Insight avec les informations d'identification du domaine Active Directory.

Cause

Les causes les plus fréquentes sont les suivantes : mots de passe expirés, informations d'identification incorrectes, problèmes de connectivité ou manque de synchronisation entre l'horloge du dispositif virtuel vRealize Log Insight et celle d'Active Directory.

Solution

- Vérifiez que vos informations d'identification sont valides, que votre mot de passe n'a pas expiré et que votre compte Active Directory n'est pas verrouillé.
- Si vous n'avez pas spécifié un domaine à utiliser pour l'authentification Active Directory, vérifiez que vous possédez un compte sur le domaine par défaut stocké dans la configuration vRealize Log Insight la plus récente à `/storage/core/loginsight/config/loginsight-config.xml#[number]` pour laquelle le `[number]` est le plus grand.
- Trouvez le fichier de configuration `/storage/core/loginsight/config/loginsight-config.xml#[number]` le plus récent pour lequel le `[number]` est le plus grand :
- Vérifiez la connectivité entre vRealize Log Insight et le serveur Active Directory.
 - Allez à la section **Authentification** dans la page **Administration** de l'interface utilisateur Web de vRealize Log Insight, indiquez vos informations d'identification, puis cliquez sur le bouton **Tester la connexion**.
 - Recherchez les éventuels messages relatifs à des problèmes avec DNS dans vRealize Log Insight `/storage/var/loginsight/runtime.log`.
- Vérifiez que l'horloge de vRealize Log Insight et celle d'Active Directory sont synchronisées.
 - Recherchez les éventuels messages relatifs à des variations d'horloge dans vRealize Log Insight `/storage/var/loginsight/runtime.log`.
 - Utilisez un serveur NTP pour synchroniser l'horloge de vRealize Log Insight et celle d'Active Directory.

SMTP ne fonctionne pas lorsque l'option STARTTLS est activée

Lorsque vous activez l'option STARTTLS lors de la configuration du serveur SMTP, les e-mails de test échouent. Pour résoudre ce problème, ajoutez au magasin d'approbations Java votre certificat SSL du serveur SMTP.

Prérequis

- Verify that you have the root user credentials to log in to the vRealize Log Insight virtual appliance.
- If you plan to connect to the vRealize Log Insight virtual appliance by using SSH, verify that TCP port 22 is open.

Procédure

- 1 Establish an SSH connection to the vRealize Log Insight vApp and log in as the root user.
- 2 Copiez le certificat SSL du serveur SMTP sur le vApp vRealize Log Insight.
- 3 Exécutez la commande suivante.

```
`/usr/java/latest/bin/keytool -import -alias certificate_name -file path_to_certificate -  
keystore /usr/java/latest/lib/security/cacerts`
```

Remarque Pour insérer les guillemets placés en début et en fin de commande, utilisez le symbole accent grave, situé sur la même touche que le symbole tilde sur un clavier anglais. N'utilisez pas de guillemets simples à la place.

- 4 Entrez le mot de passe par défaut **changeit**.
- 5 Exécutez la commande `service loginsight restart`.

Suivant

Accédez à **Administration > Smtip**, puis utilisez l'option **Envoyer l'e-mail de test** pour tester vos paramètres. Reportez-vous à [Configurer le serveur SMTP pour vRealize Log Insight](#)

La mise à niveau échoue du fait que la signature du fichier .pak ne peut pas être validée

La mise à niveau de vRealize Log Insight échoue en raison d'un fichier .pak endommagé, d'une licence expirée ou d'un espace disque insuffisant.

Problème

La mise à niveau de vRealize Log Insight échoue et vous obtenez le message d'erreur La mise à niveau a échoué. Échec de la mise à niveau : la signature du fichier PAK n'a pas pu être validée.

Cause

Cette erreur peut avoir les causes suivantes :

- Le fichier téléchargé n'est pas un fichier .pak.
- Le fichier .pak téléchargé est incomplet.
- La licence de vRealize Log Insight a expiré.
- Le système de fichiers racine du dispositif virtuel vRealize Log Insight ne dispose pas de suffisamment d'espace disque.

Solution

- Vérifiez que vous téléchargez un fichier .pak.
- Vérifiez le total de contrôle md5sum du fichier .pak sur le site de téléchargement VMware.
- Vérifiez qu'au moins une licence valide est configurée sur vRealize Log Insight.
- Connectez-vous au dispositif virtuel vRealize Log Insight et exécutez `df -h` pour vérifier l'espace disque disponible.

Remarque Ne placez pas de fichiers dans le système de fichiers racine du dispositif virtuel vRealize Log Insight.

La mise à niveau échoue en générant une erreur de serveur interne

La mise à niveau de vRealize Log Insight échoue en générant une erreur de serveur interne du fait d'un problème de connexion.

Problème

La mise à niveau de vRealize Log Insight échoue et le message d'erreur `Échec de la mise à niveau` s'affiche. Erreur de serveur interne.

Cause

Un problème de connexion est survenu entre le client et le serveur. Cela se produit, par exemple, lorsque vous tentez d'effectuer la mise à niveau à partir d'un client qui se trouve sur un WAN.

Solution

- ◆ Mettez LI à niveau à partir d'un client qui se trouve sur le même LAN que le serveur.