Prise en main de vRealize Log Insight

24 mai 2022
vRealize Log Insight 8.1

vmware®

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

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

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

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

Table des matières

Démarrage de vRealize Log Insight

Démarrage pour vRealize Log Insight fournit des informations sur le déploiement et la configuration de VMware® vRealize™Log Insight™, notamment comment dimensionner le dispositif virtuel vRealize Log Insight pour recevoir des messages de journaux.

Utilisez ces informations lorsque vous voulez planifier ou installer votre déploiement. Ces informations s'adressent aux administrateurs système Linux et Windows expérimentés qui maîtrisent les technologies de machine virtuelle et les opérations de centre de données.

Avant d'installer vRealize Log Insight

1

Pour commencer à utiliser vRealize Log Insight dans votre environnement, vous devez déployer le dispositif virtuel vRealize Log Insight et appliquer plusieurs configurations de base.

Ce chapitre contient les rubriques suivantes :

Fichiers journaux et formats d'archive pris en charge dans vRealize Log Insight

Vous pouvez utiliser vRealize Log Insight pour analyser les données de journaux structurées et non structurées.

vRealize Log Insight accepte les données à partir des sources suivantes :

- Les sources qui prennent en charge l'envoi de flux de journaux avec le protocole Syslog.
- Les sources qui écrivent les fichiers journaux et qui exécutent l'agent vRealize Log Insight.
- Les sources qui peuvent enregistrer les données des journaux avec HTTP ou HTTPS via le service REST API. La documentation de l'API est disponible depuis l'interface de vRealize Log Insight à la page `https://<vRLI_host>/rest-api`.
- Les données d'historique archivées par vRealize Log Insight.

L'analyseur de journaux vSphere vous permet d'importer des bundles de journaux vSphere dans vRealize Log Insight.

Note 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.

Reportez-vous à la section Importer une archive Log Insight dans vRealize Log Insight dans *Administration de vRealize Log Insight*.

Exigences en matière de sécurité

Pour garantir que votre environnement virtuel est protégé des attaques externes, vous devez respecter certaines règles.

- Installez toujours vRealize Log Insight dans un réseau approuvé.
- Enregistrez toujours les bundles de support de vRealize Log Insight dans un emplacement sécurisé.

Les décideurs, les architectes, les administrateurs et les autres utilisateurs du service informatique qui doivent se familiariser avec les composants de sécurité de vRealize Log Insight doivent lire les rubriques de sécurité dans *Administration de vRealize Log Insight*.

Ces rubriques fournissent des références concises vers les fonctionnalités de sécurité de vRealize Log Insight. Les rubriques traitent des interfaces externes du produit, des ports, des mécanismes d'authentification ainsi que des options de configuration et de gestion des fonctionnalités de sécurité.

Pour obtenir des informations sur la sécurisation de votre environnement virtuel, reportez-vous au *Guide de sécurité de VMware vSphere* et au Centre de sécurité sur le site Web VMware.

Compatibilité du produit

vRealize Log Insight collecte des données sur le protocole Syslog et http, peut se connecter à vCenter Server pour collecter des données d'événements, de tâches et d'alarmes et peut être intégré à vRealize Operations Manager pour envoyer des événements de notification et activer le lancement contextuel. Consultez les *Notes de mise à jour de VMware vRealize Log Insight* pour obtenir les dernières informations sur les versions du produit prises en charge.

Déploiement du dispositif virtuel

Vous devez déployer le dispositif virtuel vRealize Log Insight à l'aide de vSphere. Utilisez toujours un vSphere Client pour vous connecter à vCenter Server. Le dispositif virtuel vRealize Log Insight est déployé sur un hôte ESX/ESXi version 5.0 ou ultérieure géré par vCenter Server version 5.0 ou ultérieure.

Flux Syslog

vRealize Log Insight collecte et analyse les données syslog sur les ports et protocoles suivants.

- 514/UDP
- 514/TCP
- 1514/TCP (SSL)

Vous devez configurer des composants d'environnement tels que les systèmes d'exploitation, les applications, le stockage, les pare-feu et les périphériques réseau de manière à transmettre leurs flux syslog vers vRealize Log Insight.

Flux d'API

L'API Ingestion de vRealize Log Insight collecte les données sur les ports et les protocoles suivants.

- 9000/TCP
- 9543/TCP (SSL)

intégration de vSphere

Vous pouvez configurer vRealize Log Insight de manière à extraire les données pour les tâches, les événements et les alarmes qui se sont produits dans une ou plusieurs instances de vCenter Server. vRealize Log Insight utilise l'API vSphere pour se connecter aux systèmes vCenter Server et collecter des données.

Vous pouvez configurer des hôtes ESXi de manière à transférer les données syslog vers vRealize Log Insight.

Pour voir des informations sur la compatibilité avec des versions spécifiques de vCenter Server et ESXi, consultez les Matrices d'interopérabilité des produits VMware.

Pour plus d'informations sur la connexion à un environnement vSphere, consultez Connecter vRealize Log Insight à un environnement vSphere.

Intégration de vRealize Operations Manager

vRealize Log Insight et le vApp ou la version installable de vRealize Operations Manager peuvent être intégrés de deux manières indépendantes.

Toutes les versions prises en charge de vCenter Operations Manager prennent en charge les notifications ainsi que le lancement contextuel.

- vRealize Log Insight peut envoyer des événements de notification à vRealize Operations Manager.

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

- Le menu de lancement contextuel de vRealize Operations Manager peut afficher des actions associées à vRealize Log Insight.

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

Configuration minimale requise

VMware distribue vRealize Log Insight sous forme de dispositif virtuel dans le format de fichier OVA. Diverses ressources et applications doivent être disponibles pour garantir le bon fonctionnement du dispositif virtuel. Pour obtenir les informations actualisées sur les conditions requises, consultez les toutes dernières notes de mise à jour.

Matériel virtuel

Pendant le déploiement du dispositif virtuel vRealize Log Insight, vous pouvez choisir parmi des tailles de configuration prédéfinies conformément aux conditions 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, décrite dans le tableau suivant, consomme le moins de ressources possible tout en restant prise en charge. Une très petite configuration est également disponible, mais n'est appropriée que pour les démonstrations.

Pour connaître la configuration requise complète des ressources sur la base des exigences d'ingestion, reportez-vous à la section Dimensionnement du dispositif virtuel vRealize Log Insight

Tableau 1-1. Valeurs prédéfinies pour les petites configurations

Ressources	Configuration minimale requise
Mémoire	8 Go
vCPU	4
Espace de stockage	530 Go

Navigateurs pris en charge

Vous pouvez utiliser l'un des navigateurs suivants pour vous connecter à l'interface utilisateur Web de vRealize Log Insight. Les versions les plus récentes de navigateur sont également compatibles avec vRealize Log Insight, mais n'ont pas été validées.

Important Les cookies doivent être activés dans votre navigateur.

- Mozilla Firefox 45.0 et versions ultérieures
- Google Chrome 51.0 et versions ultérieures
- Safari 9.1 et versions ultérieures

- Internet Explorer 11.0 et versions ultérieures

Note

- Le mode document Internet Explorer doit être défini sur **Mode standard**. Les autres modes ne sont pas pris en charge.
- **Mode navigateur :** Affichage de compatibilité n'est pas pris en charge.
- Pour utiliser Internet Explorer avec le client Web vRealize Log Insight, l'intégrité du stockage local Windows doit être configurée sur le niveau Faible.

Mots de passe de comptes

Type	Configuration requise
Racine	À moins que vous ne spécifiez un mot de passe racine ou que vous n'utilisiez une personnalisation d'invité lors du déploiement du dispositif virtuel ouvert, les informations d'identification par défaut de l'utilisateur racine sur le dispositif virtuel vRealize Log Insight sont **`root/<blank>`**. Vous êtes invité à modifier le mot de passe du compte racine lorsque vous accédez pour la première fois à la console du dispositif virtuel vRealize Log Insight. **Note** Tant que vous n'avez pas défini le mot de passe racine, le SSH est désactivé.
Compte d'utilisateur	Les comptes d'utilisateur que vous créez dans vRealize Log Insight 3.3 et versions ultérieures requièrent un mot de passe fort. Ce mot de passe doit comporter au moins 8 caractères, dont un caractère en majuscule, un caractère en minuscule, un chiffre et un caractère spécial.

Configuration requise d'intégration

Produit	Configuration requise
vCenter Server	Pour récupérer des données d'événements, de tâches et d'alarmes d'un vCenter Server, vous devez fournir un ensemble d'informations d'identification d'utilisateur pour ce vCenter Server. Le rôle minimal requis pour enregistrer et annuler l'enregistrement de vRealize Log Insight avec un vCenter Server est **Lecture seule**. Le rôle doit être défini au niveau de vCenter Server et propagé aux objets enfants. Pour configurer les hôtes ESXi gérés par un vCenter Server, vRealize Log Insight requiert des privilèges supplémentaires.
vSphere ESXi	vSphere ESXi 6.0 Update 1 ou version ultérieure est nécessaire pour établir les connexions SSL à vRealize Log Insight.
vRealize Operations Manager	Pour activer les événements de notification et la fonctionnalité de lancement contextuel dans une instance de vRealize Operations Manager, vous devez fournir les informations d'identification de l'utilisateur de cette instance de vRealize Operations Manager.

Configuration requise de port réseau

Les ports réseau suivants doivent être accessibles en externe.

Port	Protocole
22/TCP	SSH
80/TCP	HTTP

Port	Protocole
443/TCP	HTTPS
514/UDP, 514/TCP	Syslog
1514/TCP	Ingestion Syslog via SSL uniquement
9000/TCP	API Ingestion de vRealize Log Insight
9543/TCP	vRealize Log Insight API Ingestion (SSL)

Planification du déploiement de vRealize Log Insight

Vous pouvez déployer vRealize Log Insight avec un nœud unique, un cluster unique ou un cluster avec redirecteurs.

Note Les équilibrages de charge externes ne sont pas pris en charge pour une utilisation avec vRealize Log Insight, notamment des clusters vRealize Log Insight.

Installation via vRealize Suite Lifecycle Manager

vRealize Suite Lifecycle Manager automatise l'installation, la configuration, la mise à niveau, les correctifs, la gestion de la configuration, la correction de la dérive et la santé des produits de Suites. Comme alternative à l'installation avec vRealize Log Insight, vous pouvez installer vRealize Log Insight via vRealize Suite Lifecycle Manager. Vous devez utiliser vRealize Suite Lifecycle Manager 1.2 ou version ultérieure et vRealize Log Insight 4.5.1 ou version ultérieure. Pour plus d'informations, reportez-vous à la documentation de vRealize Suite Lifecycle Manager.

Nœuds uniques

Une configuration vRealize Log Insight de base inclut un nœud unique. Les sources de consignation peuvent être les applications, les journaux du SE, les journaux de la machine virtuelle, les hôtes, vCenter Server, les commutateurs et les routeurs virtuels ou physiques, le matériel de stockage, etc. Les flux de journaux sont transportés vers le nœud vRealize Log Insight à l'aide de Syslog (UDP, TCP, TCP+SSL) ou de CFAPI (le protocole d'ingestion natif vRealize Log Insight sur HTTP ou HTTPS), soit directement par une application ou un concentrateur Syslog, soit par l'agent vRealize Log Insight installé sur la source.

Il est recommandé d'utiliser l'équilibrage de charge de vRealize Log Insight intégré (ILB) pour les déploiements sur un seul nœud et d'envoyer des requêtes et le trafic d'ingestion à l'équilibrage de charge intégré. Cela n'entraîne aucune capacité supplémentaire et simplifie la configuration si vous souhaitez ajouter des nœuds et créer un cluster pour un déploiement futur.

Comme meilleure pratique, n'utilisez pas de nœuds simples pour les environnements de production.

Clusters

Les environnements de production nécessitent généralement l'utilisation de clusters. Les clusters doivent répondre aux exigences suivantes :

- Tous les nœuds dans les clusters doivent être de taille identique et se trouver dans le même centre de données.
- L'équilibrage de charge intégré utilisé avec des clusters nécessite que les nœuds soient dans le même réseau L2.
- Les machines virtuelles vRealize Log Insight doivent être exclues de la protection par Pare-feu distribué VMware NSX.

  Cela s'explique par le fait que les adresses IP virtuelles des clusters utilisent un serveur virtuel Linux en mode Retour direct du serveur (LVS-DR) pour l'équilibrage de charge. Le mode Retour direct du serveur est plus efficace que le routage de tout le trafic de réponse via un seul membre du cluster. Toutefois, il ressemble également au trafic falsifié que le Pare-feu distribué NSX bloque.

Dimensionnement des clusters

Une configuration de cluster unique vRealize Log Insight peut inclure entre trois et 18 nœuds et utilise l'équilibrage de charge intégré. Un cluster nécessite un minimum de trois nœuds sains pour fonctionner correctement.

Les environnements de production nécessitent que les nœuds soient au moins de taille moyenne. Si vous prévoyez de travailler avec un nombre élevé de demandes simultanées, y compris des alertes, envisagez d'utiliser des nœuds de grande taille. Pour plus d'informations sur le dimensionnement, reportez-vous à la section Dimensionnement du dispositif virtuel vRealize Log Insight.

Bien que le nombre minimal de nœuds dans un cluster vRealize Log Insight soit de trois, si les nœuds ont échoué, un cluster avec moins de trois nœuds sains ne sera pas entièrement fonctionnel. En outre, le nombre de nœuds sains dans le cluster doit être supérieur à la moitié du nombre total de nœuds du cluster. Par exemple, si vous avez un cluster à six nœuds et que trois nœuds deviennent indisponibles, le cluster ne sera pas entièrement fonctionnel, sauf si vous supprimez les nœuds non fonctionnels du cluster. Le processus de suppression et réintroduction d'un nœud de cluster n'est pas pris en charge.

Clusters avec redirecteurs

Une configuration de cluster vRealize Log Insight avec redirecteurs inclut l'indexation principale, le stockage et un cluster de requête de 3 à 18 nœuds utilisant l'équilibrage de charge intégré. Un message de journal unique est présent dans un seul emplacement du cluster principal, comme dans le cluster unique.

La conception est étendue via l'ajout de plusieurs clusters ou clusters de redirecteurs sur les sites distants. Chaque cluster de redirecteur est configuré pour transférer tous ses messages de journaux vers le cluster principal. Les utilisateurs se connectent au cluster principal en utilisant l'API Collection Framework (cfapi) pour la compression et la résilience sur le chemin du transfert. Les clusters de redirecteurs définis comme commutateur TOR (Top-of-rack) peuvent être configurés avec une rétention locale plus importante.

Transfert croisé pour la redondance

Ce scénario de déploiement vRealize Log Insight inclut un cluster avec redirecteur étendu et mis en miroir. Deux clusters principaux sont utilisés pour l'indexation, le stockage et les requêtes. Un cluster principal figure dans chaque centre de données. Chacun d'eux est frontal avec une paire de clusters de redirecteurs dédiés. Toutes les sources de consignation de toutes les agrégations de commutateur TOR (Top-of-rack) se concentrent dans les clusters de redirecteurs. Vous pouvez interroger les mêmes journaux de manière indépendante sur les deux clusters de rétention.

Équilibrage de charge intégré vRealize Log Insight

Pour équilibrer correctement le trafic entre les nœuds d'un cluster et réduire la capacité administrative, utilisez l'équilibrage de charge intégré pour tous les déploiements. L'équilibrage de charge intégré garantit que le trafic d'ingestion entrant est accepté, même si certains nœuds vRealize Log Insight ne sont plus disponibles.

Dimensionnement du dispositif virtuel vRealize Log Insight

Par défaut, le dispositif virtuel vRealize Log Insight utilise les valeurs prédéfinies pour les petites configurations.

Déploiement autonome

Vous pouvez modifier les paramètres du dispositif afin de répondre aux besoins de l'environnement pour lequel vous prévoyez de collecter des journaux lors du déploiement.

vRealize Log Insight fournit des tailles de VM (machines virtuelles) prédéfinies que vous pouvez sélectionner 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.

Taille prédéfinie	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

Taille prédéfinie	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

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.

Le dimensionnement repose sur les hypothèses suivantes.

- Chaque CPU virtuel est d'au moins 2 GHz.
- Chaque hôte ESXi envoie jusqu'à 10 messages par seconde avec une taille moyenne de message de 170 octets/message, ce qui équivaut approximativement à 150 Mo par jour et par hôte.

Note Pour les grandes installations, vous devez mettre à niveau la version du matériel virtuel de la machine virtuelle vRealize Log Insight. vRealize Log Insight prend en charge la version 7 (ou version ultérieure) du matériel virtuel. La version 7 du matériel virtuel peut prendre en charge jusqu'à 8 CPU virtuels. Par conséquent, si vous prévoyez de provisionner 16 CPU virtuels, vous devez effectuer la mise à niveau vers la version 8 du matériel virtuel ou une version ultérieure pour ESXi 5.x. Vous utilisez vSphere Client pour mettre à niveau le matériel virtuel. Pour mettre à niveau le matériel virtuel vers la dernière version, prenez connaissance des informations de l'article Mise à niveau d'une machine virtuelle vers la dernière version matérielle (1010675) de la base de connaissances VMware.

Déploiement en cluster

Utilisez une configuration moyenne ou plus grande pour les nœuds principal et travailleur dans un cluster vRealize Log Insight. Le nombre d'événements par seconde est directement proportionnel au nombre de nœuds. Par exemple, dans un cluster de 3 à 18 nœuds (les clusters doivent comporter au moins trois nœuds), l'ingestion dans un cluster de 18 nœuds est de 270 000 événements par seconde (EPS) ou 4 To d'événements par jour.

Réduction de la taille de la mémoire

Utilisez la version **Très petite** du dispositif dans un environnement de validation technique ou de test, mais pas dans un environnement de production. Cette configuration prend en charge jusqu'à 20 hôtes ESXi (environ 200 événements/seconde ou environ 3 Go/jour).

Calculatrice de dimensionnement de vRealize Log Insight

Une calculatrice vous aide à déterminer le dimensionnement de vRealize Log Insight ainsi que l'utilisation du réseau et du stockage. Cet outil fournit des informations précieuses mais son utilisation est facultative. La plupart des valeurs d'environnement étant propres à leur site de destination, la calculatrice utilise nécessairement des estimations dans certaines zones. Reportez-vous à https://www.vmware.com/go/loginsight/calculator.

Note Les performances globales de vRealize Log Insight peuvent se dégrader si des redirecteurs sont définis par rapport au champ de texte avec des conditions complexes ou multiples impliquant des expressions régulières, par exemple « **`text=~« Suppression de la machine »`**. Dans de tels cas, en particulier lorsque la charge globale sur le cluster est élevée, cela peut avoir une incidence sur les performances. Les blocs de disques peuvent alors s'accumuler sur chaque nœud du cluster.

Intégration de vRealize Log Insight et vRealize Operations Manager

Pour activer l'intégration entre vRealize Log Insight et vRealize Operations Manager, une configuration doit être effectuée dans les deux produits.

Procédure

1. Installez vRealize Log Insight Management Pack dans vRealize Operations Manager.

   vRealize Log Insight Management Pack est requis pour la fonctionnalité de lancement contextuel entre les deux produits. vRealize Log Insight Management Pack est inclus dans le fichier de téléchargement de vRealize Operations Manager ou disponible sur le site Web de VMware Solution Exchange.

2. Configurez vRealize Log Insight pour une connexion à vRealize Operations Manager.

3. Configurez les alertes de vRealize Log Insight pour transférer les informations à vRealize Operations Manager.

   Consultez Configurer vRealize Log Insight pour qu'il envoie les événements de notification à vRealize Operations Manager dans *Administration de vRealize Log Insight*.

4. Activez la fonctionnalité lancement contextuel de vRealize Operations pour interroger les journaux dans vRealize Log Insight.

   Consultez Activer le lancement contextuel de vRealize Log Insight dans vRealize Operations Manager dans *Administration de vRealize Log Insight*.

Cycle de vie d'un événement

2

Il est impératif de comprendre la manière dont vRealize Log Insight traite les messages et les événements pour utiliser vRealize Log Insight efficacement.

Le cycle de vie d'un message de journal ou d'un événement comporte plusieurs étapes, notamment la lecture, l'analyse, l'ingestion, l'indexation, l'émission d'alertes, l'application de requête, l'archivage et la suppression.

Les événements et les messages passent par les étapes suivantes.

1 Il est généré sur un périphérique (à l'extérieur de vRealize Log Insight).

2 Il est prélevé et envoyé à vRealize Log Insight de l'une des manières suivantes :

- Par un agent vRealize Log Insight utilisant l'API Ingestion ou Syslog
- Via un agent tiers tel que rsyslog, syslog-ng ou log4j utilisant Syslog
- Par l'écriture personnalisée dans l'API Ingestion (par exemple log4j appender)
- Par l'écriture personnalisée dans Syslog (par exemple log4j appender)

3 vRealize Log Insight reçoit l'événement.

- Si vous utilisez l'équilibrage de charge intégré, l'événement est dirigé vers un nœud unique chargé de le traiter.
- Si l'événement est refusé, le client traite les refus avec des abandons UDP, TCP avec des paramètres de protocole ou CFAPI avec une file d'attente sauvegardée sur disque.
- Si l'événement est accepté, le client en est informé.

4 L'événement est transmis par le pipeline d'ingestion de vRealize Log Insight, à partir duquel les étapes suivantes sont exécutées :

- Un index de mots clés est créé ou mis à jour. L'index est stocké dans un format propriétaire sur un disque local.
- L'apprentissage de machine s'applique aux événements des clusters.
- L'événement est stocké dans un format propriétaire compressé sur le disque local dans un compartiment.

5 L'événement est interrogé.

- Les requêtes de mots clés et de globs sont comparées à l'index de mots clés.

- Regex est comparé à des événements compressés.

6 L'événement est déplacé vers un compartiment et archivé.

- Un compartiment est scellé et archivé lorsqu'il atteint 0,5 Go.

7 L'événement est supprimé.

- Les compartiments sont supprimés selon la règle du premier entré, premier sorti.

Pour en savoir plus

Pour plus d'informations, reportez-vous à la vidéo VMware Tech Pubs relative

au cycle de vie d'un événement de journal dans vRealize Log Insight. (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_horp849x/uiConfId/50138843/)

Ce chapitre contient les rubriques suivantes :

- Aspects clés du cycle de vie d'un événement

Aspects clés du cycle de vie d'un événement

Lorsqu'un événement dure, des aspects essentiels liés à son stockage et à sa gestion au cours de son cycle de vie doivent être pris en compte.

Stockage des événements

Chaque événement est stocké dans un compartiment sur disque spécifique. Lorsque vous utilisez des compartiments, tenez compte des comportements et caractéristiques suivants.

- La taille maximale des compartiments est de 0,5 Go. Lorsqu'un compartiment atteint 0,5 Go, il est scellé et en file d'attente pour l'archivage. Une fois qu'un compartiment scellé est archivé, il est marqué comme étant archivé. Un événement peut être conservé localement et dans les archives simultanément.
- Les compartiments ne sont pas répliqués entre nœuds vRealize Log Insight. Si vous perdez un nœud, vous perdez les données qui sont contenues dessus.
- Tous les compartiments sont stockés sur la partition `/storage/core`.
- vRealize Log Insight supprime les anciens compartiments lorsque l'espace disponible sur la partition `/storage/core` est inférieur à 3 %. La suppression suit le modèle « Premier entré, premier sorti ».

  Note Une partition `/storage/core` quasiment saturée est habituelle et prévue. Cette partition ne doit jamais devenir 100 % saturée, car vRealize Log Insight la gère. Toutefois, ne tentez pas de stocker des données sur cette partition, car cela peut interférer avec la suppression d'anciens compartiments.

Gestion des événements

Lorsque vous configurez votre produit, il est utile de se familiariser avec les caractéristiques suivantes, avec les comportements des événements de vRealize Log Insight et avec la gestion des événements.

- Une fois qu'un événement est supprimé localement, il ne peut plus être interrogé, sauf s'il est importé à partir de l'archive en utilisant l'interface de ligne de commande.
- Une fois que tous les événements d'un cluster d'apprentissage d'une machine ont été supprimés de vRealize Log Insight, le cluster est supprimé.
- vRealize Log Insight rééquilibre tous les événements entrants équitablement entre les nœuds du cluster. Par exemple, même si un nœud est explicitement envoyé à un événement, le nœud n'ingérera pas nécessairement l'événement.
- Les métadonnées d'événement sont stockées dans un format propriétaire sur un nœud vRealize Log Insight spécifique plutôt que dans une base de données.
- Un événement peut exister localement sur un nœud et sur l'archive.

Installation de vRealize Log Insight

3

vRealize Log Insight est livré sous la forme d'un dispositif virtuel à déployer dans votre environnement vSphere.

Après avoir examiné Dimensionnement du dispositif virtuel vRealize Log Insight, accédez à Déployer le dispositif virtuel vRealize Log Insight. Qu'il s'agisse d'un déploiement à un seul nœud ou d'un déploiement de cluster, suivez la procédure OVF standard de déploiement décrite dans cette section.

Note Vous pouvez utiliser vRealize Suite Lifecycle Manager 1.2 ou version ultérieure pour installer vRealize Log Insight 4.5.1 et versions ultérieures. Pour plus d'informations, reportez-vous à la documentation de vRealize Suite.

Ce chapitre contient les rubriques suivantes :

- Déployer le dispositif virtuel vRealize Log Insight
- Démarrer un nouveau déploiement de vRealize Log Insight
- Rejoindre un déploiement existant

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.

Conditions préalables

- 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 (machines virtuelles) prédéfinies que vous pouvez sélectionner 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.

Taille prédéfinie	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
Moyenne	75 Go/jour	8	16 Go	1 000	250	5000
Grande	225 Go/jour	16	32 Go	1 500	750	15 000

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.

Note 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.

Note 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 Sélectionner les réseaux, définissez les paramètres de mise en réseau du dispositif virtuel vRealize Log Insight. Vous pouvez sélectionner le protocole IPv4 ou IPv6.

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.

Attention 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.

Sous application, cochez la case **Préférer les adresses IPv6** pour exécuter la machine virtuelle dans un réseau à double pile.

Attention Ne cochez pas la case **Préférer les adresses IPv6** pour utiliser le protocole IPv4 pur même si IPv6 est pris en charge sur votre réseau. Cochez la case uniquement si votre réseau dispose d'une prise en charge de la double pile ou de la pile pure pour IPv6.

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 Accédez 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. 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.

Étape suivante

- Si vous souhaitez configurer un déploiement autonome de vRealize Log Insight, reportez-vous à Configurer un nouveau déploiement de Log Insight.

  L'interface Web de vRealize Log Insight est disponible à l'adresse https://*log-insight-host*/ où *log-insight-host* est l'adresse IP ou le nom d'hôte du dispositif virtuel vRealize Log Insight.

Démarrer un nouveau déploiement de vRealize Log Insight

Lorsque vous accédez à l'interface Web de vRealize Log Insight pour la première fois après le déploiement du dispositif virtuel ou après la suppression d'un nœud worker d'un cluster, vous devez terminer les étapes de configuration initiales.

Tous les paramètres que vous modifiez pendant la configuration initiale sont également disponibles dans l'interface utilisateur Web d'administration.

Pour plus d'informations sur les données de suivi que vRealize Log Insight peut collecter et envoyer à VMware lorsque vous participez au programme d'amélioration du produit, reportez-vous au Chapitre 4 Le programme d'amélioration du produit.

Conditions préalables

- Dans vSphere Client, notez l'adresse IP du dispositif virtuel vRealize Log Insight. Pour plus d'informations sur la localisation de l'adresse IP, reportez-vous à Déployer le dispositif virtuel vRealize Log Insight.
- Vérifiez que vous utilisez un navigateur pris en charge. Reportez-vous à la section Configuration minimale requise.
- Vérifiez que vous disposez d'une clé de licence valide. Vous pouvez demander une clé de licence d'évaluation ou de licence permanente via votre compte sur My VMware™ à l'adresse https://my.vmware.com/.

- Si vous souhaitez utiliser des informations d'identification locales, vCenter Server ou Active Directory pour intégrer vRealize Log Insight à vRealize Operations Manager, vérifiez que ces utilisateurs sont importés dans l'interface utilisateur personnalisée de vRealize Operations Manager. Pour obtenir des instructions sur la configuration de LDAP, reportez-vous à la documentation de vRealize Operations Manager.

Procédure

1 Utilisez un navigateur pris en charge pour naviguer dans l'interface utilisateur Web de vRealize Log Insight.

   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.

   L'assistant de configuration initiale s'ouvre.

2 Cliquez sur **Démarrer un nouveau déploiement**.

3 Définissez le mot de passe de l'utilisateur Admin et cliquez sur **Enregistrer et continuer**.

   Vous pouvez éventuellement fournir une adresse e-mail pour l'utilisateur Admin.

4 Entrez la clé de licence, cliquez sur **Ajouter une clé de licence**, puis sur **Enregistrer et continuer**.

5 Sur la page Configuration générale, entrez l'adresse e-mail qui recevra les notifications système de vRealize Log Insight.

6 Si vous utilisez des webhooks pour envoyer des notifications à vRealize Operations Manager ou à une application tierce, entrez une liste d'URL séparées par des espaces dans la zone de texte **Envoyer des notifications système HTTP Post à**.

7 (Facultatif) Pour quitter le programme d'amélioration du produit, désélectionnez l'option **Participer au programme d'amélioration du produit VMware**. Cliquez sur **Enregistrer et continuer**.

8 Dans la page Configuration de l'heure, définissez le mode de synchronisation de l'heure du dispositif virtuel vRealize Log Insight et cliquez sur **Tester**.

Option	Description
Serveur NTP (recommandé)	Par défaut, l'heure de vRealize Log Insight se synchronise avec celle de serveurs NTP publics. Si un serveur NTP externe n'est pas accessible en raison de paramètres de pare-feu, vous pouvez utiliser le serveur NTP interne de votre organisation. Utilisez des virgules pour séparer plusieurs serveurs NTP.
Hôte ESX/ESXi	Si aucun serveur NTP n'est disponible, vous pouvez synchroniser l'heure avec l'hôte ESXi sur lequel vous avez déployé le dispositif virtuel vRealize Log Insight.

9 Cliquez sur **Enregistrer et continuer**.

10 (Facultatif) Pour activer les alertes sortantes et les e-mails de notification système, spécifiez les propriétés d'un serveur SMTP.

   Pour vérifier que la configuration SMTP est correcte, entrez une adresse e-mail valide, puis cliquez sur **Tester**.vRealize Log Insight envoie un e-mail de test à l'adresse que vous avez fournie.

11 (Facultatif) Pour fournir un certificat SSL personnalisé, téléchargez un fichier de certificat vers le cluster au format PEM. Vous pouvez également afficher les détails du certificat existant.

   Le système ajoute le certificat aux magasins d'approbations de tous les nœuds du cluster et l'enregistre pour une utilisation ultérieure.

   Pour plus d'informations sur les conditions préalables du certificat SSL personnalisé, reportez-vous à la section Installer un certificat SSL personnalisé.

12 Cliquez sur **Enregistrer et continuer**.

Résultats

Après le redémarrage du processus vRealize Log Insight, vous êtes dirigé vers l'onglet **Tableaux de bord** de vRealize Log Insight.

Étape suivante

- Accédez à l'onglet **Administration**. Sur la page **Intégration vSphere**, configurez vRealize Log Insight de manière qu'il extraie les tâches, événements et alertes provenant des instances de vCenter Server et à ce qu'il configure les hôtes ESXi pour qu'ils envoient les flux Syslog à vRealize Log Insight.
- Attribuez une licence permanente à vRealize Log Insight. Reportez-vous à la section Attribuer une licence permanente à Log Insight dans *Administration de vRealize Log Insight.*
- Configurez l'adaptateur vRealize Log Insight dans vRealize Operations Manager pour activer le lancement contextuel. Consultez la section *Configuration de vRealize Log Insight avec vRealize Operations Manager* dans le *Guide de configuration de vRealize Operations Manager*.
- Installez l'agent Windows de vRealize Log Insight pour collecter des événements provenant de canaux d'événements Windows, de répertoires Windows et de fichiers journaux texte plats. Consultez la section Installation des agents Windows dans *Utilisation des agents vRealize Log Insight*.

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 de cluster, vRealize Log Insight fournit des nœuds principal et travailleur. Ces deux types de nœuds sont responsables d'un sous-ensemble de données. Les nœuds principaux peuvent interroger tous les sous-ensembles de données et agréger les résultats. Vous pouvez avoir besoin de davantage de nœuds pour répondre aux besoins du site. Vous pouvez utiliser entre trois et 18 nœuds dans un cluster. Cela signifie qu'un cluster entièrement fonctionnel doit disposer d'un minimum de trois nœuds sains. La plupart des nœuds d'un cluster de taille supérieure doivent être sains. Par exemple, si les trois nœuds d'un cluster de nœuds six échouent, aucun des nœuds ne fonctionne complètement tant que les nœuds ayant échoué n'ont pas été supprimés.

Conditions préalables

- 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 d'hôte du dispositif virtuel vRealize Log Insight principal.
- Vérifiez que vous disposez d'un compte d'administrateur sur le dispositif virtuel vRealize Log Insight principal.
- Vérifiez que les versions des nœuds principal et travailleur de vRealize Log Insight sont synchronisées. N'ajoutez pas un travailleur vRealize Log Insight de version antérieure à un nœud principal vRealize Log Insight de version plus récente.
- 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 travailleur vRealize Log Insight.

   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 nœud principal de vRealize Log Insight, puis cliquez sur **Aller à**.

   Le travailleur envoie au nœud principal de vRealize Log Insight 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 nœud worker rejoint le déploiement existant et vRealize Log Insight commence à fonctionner dans un cluster.

Étape suivante

- Ajoutez davantage de nœuds worker en fonction des besoins. Le cluster doit contenir au moins trois nœuds.

Le programme d'amélioration du produit

4

Ce produit participe au Programme d'amélioration du produit (CEIP) de VMware.

Les détails relatifs aux données recueillies grâce au CEIP et les fins auxquelles elles sont utilisées par VMware sont énoncés par le Trust & Assurance Center, à l'adresse https://www.vmware.com/solutions/trustvmware/ceip.html.

Pour participer au programme d'amélioration du produit (CEIP) pour ce produit ou pour le quitter, reportez-vous à la rubrique indiquant comment rejoindre ou quitter le programme d'amélioration du produit VMware dans *Administration de vRealize Log Insight*.