

Utilisation de l'importateur de vRealize Log Insight

28 novembre 2019

vRealize Log Insight 8.0



vmware®

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

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

Si vous avez des commentaires à propos de cette documentation, envoyez-les à l'adresse suivante :

docfeedback@vmware.com

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

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

Copyright © 2019 VMware, Inc. Tous droits réservés. [Informations relatives aux copyrights et marques commerciales.](#)

Table des matières

1	Utilisation de vRealize Log Insight Importer	4
	Installation de vRealize Log Insight Importer	4
	Avant d'installer l'vRealize Log Insight Importer	5
	Installer vRealize Log Insight Importer	5
	Exécution de vRealize Log Insight Importer	6
	À propos du fichier de manifeste de vRealize Log Insight Importer	7
	Exemples de configuration de fichier de manifeste vRealize Log Insight Importer	7
	Exécuter vRealize Log Insight Importer	8

Utilisation de vRealize Log Insight Importer

1

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.

Utilisez l'importateur lorsque vous souhaitez importer des journaux qui ont été collectés antérieurement. Vous pouvez importer des bundles de support et des journaux archivés et analyser les journaux des bundles de support collectés à partir de vRealize Log Insight ou tout autre 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 de fichier, y compris la collecte de répertoires récurifs.
- L'importateur peut lire les données de fichiers d'archives aux formats zip, tar, bzip, bzip2 ou gz. 7-Zip n'est pas pris en charge.
- Vous pouvez spécifier que les données soient lues de manière récursive à partir d'une archive imbriquée (par ex., un fichier ZIP imbriqué), ou depuis un répertoire au sein d'une archive.

Ce chapitre contient les rubriques suivantes :

- [Installation de vRealize Log Insight Importer](#)
- [Exécution de vRealize Log Insight Importer](#)

Installation de vRealize Log Insight Importer

Vous installez l'importateur de vRealize Log Insight à partir d'un module d'installation que vous obtenez sur le site de téléchargement VMware. Les modules d'installation incluent le programme d'installation MSI pour Windows et les modules d'installation POSIX (RPM, DEB et BIN) pour Linux.

- [Avant d'installer l'vRealize Log Insight Importer](#)

Vérifiez la configuration requise et comprenez le comportement de l'importateur avant de l'installer.

- [Installer 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.

Avant d'installer l'vRealize Log Insight Importer

Vérifiez la configuration requise et comprenez le comportement de l'importateur avant de l'installer.

Avant l'installation, vérifiez 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.

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.

Lorsque vous utilisez l'importateur, vous devez connaître les comportements suivants :

- 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.

Installer 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.

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, supprimez également le lien symbolique /usr/bin/loginsight_importer.

Conditions préalables

- Vérifiez que vous pouvez accéder au site de [téléchargement VMware](#) pour télécharger vRealize Log Insight Importer.

Procédure

- 1 Téléchargez le module d'installation vRealize Log Insight Importer sur le site de [téléchargement VMware](#).

Les modules d'installation incluent le programme d'installation MSI pour Windows et les modules d'installation POSIX (RPM, DEB et BIN) pour Linux.

- 2 Installez l'outil sur votre système.

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 le fichier 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.

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

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

Exécution de vRealize Log Insight Importer

Lorsque vous exécutez l'importateur, vous devez inclure un fichier manifeste. Le fichier manifeste fournit des informations sur le format des journaux, l'emplacement des données à importer et sur la source et la destination.

- [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.
- [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.
- [Exécuter vRealize Log Insight Importer](#)
Exécutez vRealize Log Insight Importer pour importer des journaux hors ligne de données historiques sur le serveur vRealize Log Insight.

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 éventuellement créer votre propre fichier de manifeste pour importer des fichiers journaux arbitraires. L'un des avantages de la création d'un fichier de ce type est que 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*`), puis 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 plus d'informations sur les options prises en charge dans la section `[filelog]` et pour voir des exemples de configuration, consultez la rubrique « Collecter des événements depuis un fichier journal » dans la section *Utilisation d'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 vRealize Log Insight Importer considère le chemin d'accès 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.

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_channel3]
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
```

Exécuter vRealize Log Insight Importer

Exécutez vRealize Log Insight Importer pour importer des journaux hors ligne de données historiques sur le serveur vRealize Log Insight.

Conditions préalables

- 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](#).
- 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, configurez le paramètre `honor_timestamp`, ainsi que le nom d'utilisateur et le mot passe.

Procédure

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

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

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

Les paramètres `--source` et `--server` sont obligatoires.

Paramètres requis	Description
<code>--source <chemin></code>	Spécifie le chemin vers un répertoire de bundle de support ou le chemin vers une archive zip, gzip, bzip, bzip2 ou tar. La valeur est ajoutée à tous les messages envoyés comme valeur de la balise bundle.
<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.

Options	Description
<code>--tags <balises></code>	<p>Définir les balises pour tous les événements envoyés. Par exemple, <code>--tags "{ \"balise1\" : \"valeur1\", \"balise2\": \"valeur2\"}"</code></p> <p>Note L'option tags peut accepter hostname comme nom de balise. La valeur de la balise hostname de la ligne de commande est utilisée à la place du nom de domaine complet de la machine émettrice comme valeur du champ hostname pour tous les événements extraits par vRealize Log Insight Importer. C'est le contraire du paramètre tags du fichier de manifeste et des champs extraits par les analyseurs, qui ignorent le champ hostname.</p> <p>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 bundle 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 bundle remplace les balises avec le même nom dans un fichier manifeste. Elle peut cependant être remplacée par des balises de ligne de commande, s'il en existe une avec le nom bundle.</p>
<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 username/password désactive le décalage de temps autorisé sur le serveur vRealize Log Insight afin de rendre possible l'importation des données avec un horodatage historique.
<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>Note 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.

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

vRealize Log Insight Importer extrait 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.

Étape suivante

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.