

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

Verwalten von vRealize Log Insight	7
Updated Information for <i>Verwalten von vRealize Log Insight</i>	8
1 Aktualisieren von vRealize Log Insight	9
Upgrade-Pfad für vRealize Log Insight	9
Upgrade auf vRealize Log Insight 4.5	10
Upgrade auf vRealize Log Insight 4.3	11
Upgrade auf vRealize Log Insight 4.0	12
Upgrade auf vRealize Log Insight 3.6	13
2 Verwalten von vRealize Log Insight-Benutzerkonten	15
Benutzerverwaltung – Übersicht	16
Rollenbasierte Zugriffssteuerung	16
Erstellen eines neuen Benutzerkontos in vRealize Log Insight	17
Konfigurieren des VMware Identity Manager -Zugriffs auf Active Directory-Gruppen für vRealize Log Insight	18
Importieren einer Active Directory-Gruppe in vRealize Log Insight	20
Authentifizieren von Benutzern mit domänenübergreifender Gruppen-Mitgliedschaft	21
Definieren eines Datensatzes	22
Erstellen und Ändern von Rollen	23
Löschen eines Benutzerkontos aus vRealize Log Insight	24
3 Konfigurieren der Authentifizierung	25
Aktivieren der Benutzerauthentifizierung über VMware Identity Manager	25
Aktivieren der Benutzerauthentifizierung über Active Directory	27
Konfigurieren des für Active Directory zu verwendenden Protokolls	28
4 Konfigurieren von vRealize Log Insight	30
vRealize Log Insight Grenzwerte für die Konfiguration	31
Konfigurieren der Einstellungen für die virtuelle Appliance	32
SSH-Root-Kennwort für die virtuelle vRealize Log Insight -Appliance konfigurieren	32
Ändern der Netzwerkeinstellungen der vApp für vRealize Log Insight	33
Erhöhen der Speicherkapazität der virtuellen vRealize Log Insight -Appliance	34
Hinzufügen von Arbeitsspeicher und CPU zur virtuellen vRealize Log Insight -Appliance	36
Zuweisen einer permanenten Lizenz zu vRealize Log Insight	36
Protokollspeicherrichtlinie	37

Verwalten von Systembenachrichtigungen	37
vRealize Log Insight-Systembenachrichtigungen	38
Konfigurieren von vRealize Log Insight -Systembenachrichtigungen	48
Hinzufügen eines Ziels für die vRealize Log Insight -Ereignisweiterleitung	51
Konfigurieren der vRealize Log Insight -Ereignisweiterleitung mit SSL	54
Synchronisieren der Uhrzeit der virtuellen vRealize Log Insight -Appliance	55
Konfigurieren des SMTP-Servers für vRealize Log Insight	56
Installieren eines benutzerdefinierten SSL-Zertifikats	57
Generieren eines selbstsignierten Zertifikats	59
Generieren einer Zertifizierungsanforderung	60
Anfordern einer Signatur von einer Zertifizierungsstelle	61
Verketteten von Zertifikatsdateien	61
Hochladen des signierten Zertifikats	62
Konfigurieren der SSL-Verbindung zwischen dem vRealize Log Insight -Server und den Log Insight Agents	63
Ändern des Standard-Zeitlimits für vRealize Log Insight -Websitzungen	66
Archive	67
Aktivieren oder Deaktivieren der Datenarchivierung in vRealize Log Insight	67
Format der vRealize Log Insight -Archivdateien	68
Importieren eines vRealize Log Insight -Archivs in vRealize Log Insight	69
Exportieren eines Log Insight-Archivs in eine Rohtextdatei oder JSON	70
Neustart des vRealize Log Insight -Dienstes	71
Ausschalten der virtuellen vRealize Log Insight -Appliance	72
Herunterladen eines Support-Pakets für vRealize Log Insight	72
Teilnahme am VMware-Programm zur Verbesserung der Benutzerfreundlichkeit oder Verlassen des Programms	73
5 Konfigurieren von vRealize Log Insight-Clustern	75
Hinzufügen eines Worker-Knotens zu einem vRealize Log Insight -Cluster	75
Bereitstellen der virtuellen vRealize Log Insight -Appliance	76
Hinzufügen zu einer vorhandenen Bereitstellung	79
Entfernen eines Worker-Knotens aus einem vRealize Log Insight -Cluster	80
Arbeiten mit einem integrierten Lastausgleichsdienst	81
Aktivieren des integrierten Lastausgleichsdienstes	82
Abfragen der Ergebnisse von Clusterprüfungen in der Produktion	83
6 Ports und externe Schnittstellen	85
7 Überwachen des Status von vRealize Log Insight Windows- und Linux-Agenten	89
8 Aktivieren der automatischen Agent-Aktualisierung vom Server	90

9	Arbeiten mit Agentengruppen	91
	Zusammenführen von Agentengruppen-Konfigurationen	92
	Erstellen einer Agentengruppe	92
	Bearbeiten einer Agentengruppe	93
	Hinzufügen einer Inhaltspaket-Agentengruppe als Agentengruppe	94
	Löschen einer Agentengruppe	94
10	Konfigurieren und Verwenden von vRealize Log Insight Importer	96
	Informationen zur vRealize Log Insight Importer -Manifestdatei	97
	Installieren, Konfigurieren und Ausführen von vRealize Log Insight Importer	98
	Beispiele für die Konfiguration von vRealize Log Insight Importer -Manifestdateien	100
	vRealize Log Insight Importer -Konfigurationsparameter	101
11	Überwachen von vRealize Log Insight	103
	Prüfen des Systemzustands der virtuellen vRealize Log Insight -Appliance	103
	Überwachen von Protokollereignisse sendenden Hosts	104
12	Integration von vRealize Log Insight in VMware-Produkte	105
	Verbinden von vRealize Log Insight mit einer vSphere-Umgebung	106
	vRealize Log Insight als Syslog-Server	108
	Konfigurieren eines ESXi -Hosts für die Weiterleitung von Protokollereignissen an vRealize Log Insight	108
	Ändern einer ESXi -Hostkonfiguration für die Weiterleitung von Protokollereignissen an vRealize Log Insight	110
	vRealize Log Insight -Benachrichtigungsereignisse in vRealize Operations Manager	111
	Konfigurieren von vRealize Log Insight für das Abrufen von Ereignissen, Aufgaben und Warnungen aus vCenter Server -Instanzen	112
	Verwenden von vRealize Operations Manager mit vRealize Log Insight	113
	Anforderungen für die Integration in vRealize Operations Manager	113
	Konfigurieren von vRealize Log Insight zum Senden von Benachrichtigungsereignissen an vRealize Operations Manager	115
	Aktivieren des kontextbezogenen Starts für vRealize Log Insight in vRealize Operations Manager	116
	Deaktivieren des kontextbezogenen Starts für vRealize Log Insight in vRealize Operations Manager	121
	Hinzufügen von DNS-Suchpfad und -domäne	122
	Entfernen des vRealize Log Insight -Adapters	123
	vRealize Operations Manager -Inhaltspaket für vRealize Log Insight	124
13	Sicherheitsüberlegungen für vRealize Log Insight	125
	Ports und externe Schnittstellen	125

vRealize Log Insight -Konfigurationsdateien	129
Öffentlicher Schlüssel, Zertifikat und Keystore für vRealize Log Insight	129
vRealize Log Insight -Lizenz und EULA-Datei	130
vRealize Log Insight -Protokolldateien	130
vRealize Log Insight Benutzerkonten	132
vRealize Log Insight -Firewall-Empfehlungen	133
Sicherheits-Updates und Patches	134

14 Sichern, Wiederherstellen und die Notfallwiederherstellung 135

Sicherung, Wiederherstellung und Notfallwiederherstellung – Überblick	135
Verwenden von statischen IP-Adressen und FQDN	136
Planung und Vorbereitung	137
Sichern von Knoten und Clustern	138
Sichern von Linux- bzw. Windows-Agents	139
Wiederherstellen von Knoten und Clustern	140
Ändern von Konfigurationen nach der Wiederherstellung	141
Wiederherstellen auf demselben Host	141
Wiederherstellen auf einem anderen Host	142
Überprüfen der Wiederherstellungen	145
Notfallwiederherstellung	146

15 Fehlerbehebung bei vRealize Log Insight 147

vRealize Log Insight steht zu wenig Festplattenspeicher zur Verfügung	147
Scheitern des Imports archivierter Daten	148
Erstellen eines Support-Pakets von vRealize Log Insight über die Virtual Appliance-Konsole	148
Zurücksetzen des Admin-Benutzerkennworts	149
Zurücksetzen des Root-Benutzerkennworts	150
Warnungen konnten nicht an vRealize Operations Manager gesendet werden	151
Anmeldung unter Verwendung der Active Directory-Anmeldedaten nicht möglich	152
SMTP funktioniert bei aktivierter STARTTLS-Option nicht	153
Fehlschlagen des Upgrades, weil die Signatur der PAK-Datei nicht validiert werden kann	154
Fehlschlagen des Upgrades mit einem internen Serverfehler	154

Verwalten von vRealize Log Insight

Verwalten von vRealize Log Insight enthält Informationen zur Verwaltung von VMware® vRealize™ Log Insight™, unter anderem zur Pflege von Benutzerkonten und zur Integration von Log Insight Agents in andere VMware-Produkte. Das Handbuch enthält auch Informationen zur Verwaltung der Produktsicherheit und zum Upgrade Ihrer Bereitstellung.

Die Informationen sind für erfahrene Systemadministratoren bestimmt, die mit der Windows- oder Linux-VM-Technologie und Datacenteroperationen vertraut sind.

Updated Information for *Verwalten von vRealize Log Insight*

Verwalten von vRealize Log Insight is updated with each release of the product or when necessary.

This table provides the update history of *Verwalten von 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 Arbeiten mit einem integrierten Lastausgleichsdienst and Chapter 3 Konfigurieren der Authentifizierung.
002541-0	Initial release.

Aktualisieren von vRealize Log Insight

1

Je nach der aktuellen Version von vRealize Log Insight können Sie auf eine neuere Version aktualisieren.

Dieses Kapitel behandelt die folgenden Themen:

- [Upgrade-Pfad für vRealize Log Insight](#)
- [Upgrade auf vRealize Log Insight 4.5](#)
- [Upgrade auf vRealize Log Insight 4.3](#)
- [Upgrade auf vRealize Log Insight 4.0](#)
- [Upgrade auf vRealize Log Insight 3.6](#)

Upgrade-Pfad für vRealize Log Insight

Der Upgrade-Pfad und -Vorgang hängt von der installierten Version von vRealize Log Insight ab, bei der Sie ein Upgrade durchführen möchten.

Sie können auch unterstützte Upgrade-Pfade prüfen, indem Sie die Funktion **Upgrade-Pfad** auf der Website mit den [VMware-Produkt-Interoperabilitätstabellen](#) verwenden.

vRealize Log Insight-Upgrades erfolgen schrittweise. Sie müssen auf jede Zwischenversion ein Upgrade durchführen.

Tabelle 1-1. Unterstützte Upgrade-Pfade

Upgrade von	Upgrade auf	Vorgehensweise
vRealize Log Insight 4.3	vRealize Log Insight 4.5	Siehe Upgrade auf vRealize Log Insight 4.5 .
vRealize Log Insight 4.0	vRealize Log Insight 4.3	Siehe Upgrade auf vRealize Log Insight 4.3 .
vRealize Log Insight 3.6	vRealize Log Insight 4.0	Weitere Informationen hierzu finden Sie unter Upgrade auf vRealize Log Insight 4.0 .
vRealize Log Insight 3.3	vRealize Log Insight 3.6	Weitere Informationen hierzu finden Sie unter Upgrade auf vRealize Log Insight 3.6 .

Upgrade auf vRealize Log Insight 4.5

Sie können einen Cluster automatisch auf vRealize Log Insight 4.5 aktualisieren.

Das Upgrade von vRealize Log Insight muss über den FQDN des Masterknotens vorgenommen werden. Das Durchführen eines Upgrades mithilfe der IP-Adresse des integrierten Lastenausgleichsdiensts wird nicht unterstützt.


Der Masterknoten wird während des Upgrades als erstes aktualisiert und dann neu gestartet. Anschließend werden alle Clusterknoten sequenziell aktualisiert. Sie können den aktuellen Status des laufenden Upgrades über die Seite **Admin > Cluster** verfolgen. Wenn der integrierte Lastenausgleichsdienst konfiguriert wird, werden dessen IPs mit den Clusterknoten migriert, sodass Clusterdienste wie die Benutzeroberfläche, API und die Erfassung eingehender Ereignisse während des laufenden Upgrades verfügbar bleiben. Details auf unterster Ebene werden für jeden einzelnen Knoten in die `upgrade.log`-Datei geschrieben. Nach erfolgreichem Abschluss des Upgrades wird eine Systemnachricht versendet.

Tritt während des Upgradeprozesses bei einem oder mehreren Knoten ein Problem auf, wird der gesamte Cluster automatisch auf die ursprüngliche, funktionierende Version zurückgesetzt. Da Konfigurationsänderungen, die nach Beginn des Upgrades vorgenommen wurden, inkonsistent oder ungültig sein können, wird die Konfiguration auf einen bekanntermaßen funktionsfähigen Zustand vor dem Upgrade zurückgesetzt. Dabei gehen keine erfassten Ereignisse verloren. Der Fortschritt wird für jeden einzelnen Knoten in die `rollback.log`-Datei geschrieben. Nach Abschluss der Wiederherstellung wird eine Systemnachricht versendet. Nachdem das Problem untersucht und behoben wurde, können Sie nochmals versuchen, ein Upgrade durchzuführen.

Voraussetzungen

- Achten Sie darauf, dass Sie das Upgrade über einen unterstützten Upgrade-Pfad durchführen. Weitere Informationen hierzu finden Sie unter [Upgrade-Pfad für vRealize Log Insight](#).
- Create a snapshot or backup copy of the vRealize Log Insight virtual appliance.
- Fordern Sie eine Kopie der `vRealize Log Insight.pak`-Datei für das Upgrade-Paket für die Version, auf die Sie ein Upgrade durchführen, an.
- 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.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Cluster**.
- 3 Klicken Sie auf **PAK hochladen**, um die `.pak`-Datei hochzuladen.
- 4 Accept the new EULA to complete the upgrade procedure.

Weiter

Nach Abschluss des Masterknoten-Upgrades können Sie den verbleibenden automatischen Upgrade-Vorgang beobachten.

Achten Sie auf die an den Administrator gesendete E-Mail, die den erfolgreichen Abschluss des Upgrades bestätigt.

Upgrade auf vRealize Log Insight 4.3

Sie können einen Cluster automatisch auf vRealize Log Insight 4.3 aktualisieren.

Das Upgrade von vRealize Log Insight muss über den FQDN des Masterknotens vorgenommen werden. Das Durchführen eines Upgrades mithilfe der IP-Adresse des integrierten Lastenausgleichsdiensts wird nicht unterstützt.

Der Masterknoten wird während des Upgrades als erstes aktualisiert und dann neu gestartet. Anschließend werden alle Clusterknoten sequenziell aktualisiert. Sie können den aktuellen Status des laufenden Upgrades über die Seite **Admin > Cluster** verfolgen. Wenn der integrierte Lastenausgleichsdienst konfiguriert wird, werden dessen IPs mit den Clusterknoten migriert, sodass Clusterdienste wie die Benutzeroberfläche, API und die Erfassung eingehender Ereignisse während des laufenden Upgrades verfügbar bleiben. Details auf unterster Ebene werden für jeden einzelnen Knoten in die `upgrade.log`-Datei geschrieben. Nach erfolgreichem Abschluss des Upgrades wird eine Systemnachricht versendet.

Tritt während des Upgradeprozesses bei einem oder mehreren Knoten ein Problem auf, wird der gesamte Cluster automatisch auf die ursprüngliche, funktionierende Version zurückgesetzt. Da Konfigurationsänderungen, die nach Beginn des Upgrades vorgenommen wurden, inkonsistent oder ungültig sein können, wird die Konfiguration auf einen bekanntermaßen funktionsfähigen Zustand vor dem Upgrade zurückgesetzt. Dabei gehen keine erfassten Ereignisse verloren. Der Fortschritt wird für jeden einzelnen Knoten in die `rollback.log`-Datei geschrieben. Nach Abschluss der Wiederherstellung wird eine Systemnachricht versendet. Nachdem das Problem untersucht und behoben wurde, können Sie nochmals versuchen, ein Upgrade durchzuführen.

Voraussetzungen

- Achten Sie darauf, dass Sie das Upgrade über einen unterstützten Upgrade-Pfad durchführen. Weitere Informationen hierzu finden Sie unter [Upgrade-Pfad für vRealize Log Insight](#).
- Create a snapshot or backup copy of the vRealize Log Insight virtual appliance.
- Fordern Sie eine Kopie der `vRealize Log Insight.pak`-Datei für das Upgrade-Paket für die Version, auf die Sie ein Upgrade durchführen, an.
- 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.

Vorgehensweise

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

- 2 Under Management, click **Cluster**.
- 3 Klicken Sie auf **PAK hochladen**, um die .pak-Datei hochzuladen.
- 4 Accept the new EULA to complete the upgrade procedure.

Weiter

Nach Abschluss des Masterknoten-Upgrades können Sie den verbleibenden automatischen Upgrade-Vorgang beobachten.

Achten Sie auf die an den Administrator gesendete E-Mail, die den erfolgreichen Abschluss des Upgrades bestätigt.

Upgrade auf vRealize Log Insight 4.0

Sie können einen Cluster automatisch auf vRealize Log Insight 4.0 aktualisieren.

Das Upgrade von vRealize Log Insight muss über den FQDN des Masterknotens vorgenommen werden. Das Durchführen eines Upgrades mithilfe der IP-Adresse des integrierten Lastausgleichsdiensts wird nicht unterstützt.

Der Masterknoten wird während des Upgrades als erstes aktualisiert und dann neu gestartet. Anschließend werden alle Clusterknoten sequenziell aktualisiert. Sie können den aktuellen Status des laufenden Upgrades über die Seite **Admin > Cluster** verfolgen. Wenn der integrierte Lastenausgleichsdienst konfiguriert wird, werden dessen IPs mit den Clusterknoten migriert, sodass Clusterdienste wie die Benutzeroberfläche, API und die Erfassung eingehender Ereignisse während des laufenden Upgrades verfügbar bleiben. Details auf unterster Ebene werden für jeden einzelnen Knoten in die upgrade.log-Datei geschrieben. Nach erfolgreichem Abschluss des Upgrades wird eine Systemnachricht versendet.


Tritt während des Upgradeprozesses bei einem oder mehreren Knoten ein Problem auf, wird der gesamte Cluster automatisch auf die ursprüngliche, funktionierende Version zurückgesetzt. Da Konfigurationsänderungen, die nach Beginn des Upgrades vorgenommen wurden, inkonsistent oder ungültig sein können, wird die Konfiguration auf einen bekanntermaßen funktionsfähigen Zustand vor dem Upgrade zurückgesetzt. Dabei gehen keine erfassten Ereignisse verloren. Der Fortschritt wird für jeden einzelnen Knoten in die rollback.log-Datei geschrieben. Nach Abschluss der Wiederherstellung wird eine Systemnachricht versendet. Nachdem das Problem untersucht und behoben wurde, können Sie nochmals versuchen, ein Upgrade durchzuführen.

Voraussetzungen

- Achten Sie darauf, dass Sie das Upgrade über einen unterstützten Upgrade-Pfad durchführen. Weitere Informationen hierzu finden Sie unter [Upgrade-Pfad für vRealize Log Insight](#).
- Create a snapshot or backup copy of the vRealize Log Insight virtual appliance.
- Fordern Sie eine Kopie der vRealize Log Insight.pak-Datei für das Upgrade-Paket für die Version, auf die Sie ein Upgrade durchführen, an.

- 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.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Cluster**.
- 3 Klicken Sie auf **PAK hochladen**, um die .pak-Datei hochzuladen.
- 4 Accept the new EULA to complete the upgrade procedure.

Weiter

Nach Abschluss des Masterknoten-Upgrades können Sie den verbleibenden automatischen Upgrade-Vorgang beobachten.

Achten Sie auf die an den Administrator gesendete E-Mail, die den erfolgreichen Abschluss des Upgrades bestätigt.

Upgrade auf vRealize Log Insight 3.6

Sie können einen Cluster automatisch auf vRealize Log Insight 3.6 aktualisieren.

Das Upgrade von vRealize Log Insight muss über den FQDN des Masterknotens vorgenommen werden. Das Durchführen eines Upgrades mithilfe der IP-Adresse des integrierten Lastenausgleichsdiensts wird nicht unterstützt.


Der Masterknoten wird während des Upgrades als erstes aktualisiert und dann neu gestartet. Anschließend werden alle Clusterknoten sequenziell aktualisiert. Sie können den aktuellen Status des laufenden Upgrades über die Seite **Admin > Cluster** verfolgen. Wenn der integrierte Lastenausgleichsdienst konfiguriert wird, werden dessen IPs mit den Clusterknoten migriert, sodass Clusterdienste wie die Benutzeroberfläche, API und die Erfassung eingehender Ereignisse während des laufenden Upgrades verfügbar bleiben. Details auf unterster Ebene werden für jeden einzelnen Knoten in die `upgrade.log`-Datei geschrieben. Nach erfolgreichem Abschluss des Upgrades wird eine Systemnachricht versendet.

Tritt während des Upgradeprozesses bei einem oder mehreren Knoten ein Problem auf, wird der gesamte Cluster automatisch auf die ursprüngliche, funktionierende Version zurückgesetzt. Da Konfigurationsänderungen, die nach Beginn des Upgrades vorgenommen wurden, inkonsistent oder ungültig sein können, wird die Konfiguration auf einen bekanntermaßen funktionsfähigen Zustand vor dem Upgrade zurückgesetzt. Dabei gehen keine erfassten Ereignisse verloren. Der Fortschritt wird für jeden einzelnen Knoten in die `rollback.log`-Datei geschrieben. Nach Abschluss der Wiederherstellung wird eine Systemnachricht versendet. Nachdem das Problem untersucht und behoben wurde, können Sie nochmals versuchen, ein Upgrade durchzuführen.

Voraussetzungen

- Achten Sie darauf, dass Sie das Upgrade über einen unterstützten Upgrade-Pfad durchführen. Weitere Informationen hierzu finden Sie unter [Upgrade-Pfad für vRealize Log Insight](#).
- Create a snapshot or backup copy of the vRealize Log Insight virtual appliance.
- Fordern Sie eine Kopie der vRealize Log Insight .pak-Datei für das Upgrade-Paket für die Version, auf die Sie ein Upgrade durchführen, an.
- 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.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Cluster**.
- 3 Klicken Sie auf **PAK hochladen**, um die .pak-Datei hochzuladen.
- 4 Accept the new EULA to complete the upgrade procedure.

Weiter

Nach Abschluss des Masterknoten-Upgrades können Sie den verbleibenden automatischen Upgrade-Vorgang beobachten.

Achten Sie auf die an den Administrator gesendete E-Mail, die den erfolgreichen Abschluss des Upgrades bestätigt.

Verwalten von vRealize Log Insight-Benutzerkonten

2

Administratoren können Benutzerkonten und Rollen erstellen, um Zugriff auf die Web-Benutzeroberfläche von vRealize Log Insight zu ermöglichen.

Nur Benutzer mit der Berechtigung Admin bearbeiten können Benutzerkonten erstellen und bearbeiten. Benutzer können allerdings ohne die Berechtigung Admin bearbeiten ihr eigenes E-Mail- und Kontokennwort ändern.

Dieses Kapitel behandelt die folgenden Themen:

- [Benutzerverwaltung – Übersicht](#)
- [Rollenbasierte Zugriffssteuerung](#)
- [Erstellen eines neuen Benutzerkontos in vRealize Log Insight](#)
- [Konfigurieren des VMware Identity Manager-Zugriffs auf Active Directory-Gruppen für vRealize Log Insight](#)
- [Importieren einer Active Directory-Gruppe in vRealize Log Insight](#)
- [Authentifizieren von Benutzern mit domänenübergreifender Gruppen-Mitgliedschaft](#)
- [Definieren eines Datensatzes](#)
- [Erstellen und Ändern von Rollen](#)
- [Löschen eines Benutzerkontos aus vRealize Log Insight](#)

Benutzerverwaltung - Übersicht

Systemadministratoren nutzen eine Kombination aus Benutzeranmeldungen, einer rollenbasierten Zugriffssteuerung, Berechtigungen und Datensätzen zur Verwaltung von vRealize Log Insight-Benutzern. Mit der rollenbasierten Zugriffssteuerung können Administratoren Benutzer und die Aufgaben, die diese wahrnehmen, verwalten.

Bei den Rollen handelt es sich um Berechtigungssätze, die zur Durchführung bestimmter Aufgaben erforderlich sind. Systemadministratoren definieren Rollen als Teil der Definition von Sicherheitsrichtlinien und weisen die Rollen dann den Benutzern zu. Zum Ändern der Berechtigungen und der Aufgaben, die einer bestimmten Rolle zugewiesen sind, aktualisiert der Systemadministrator die Rolleneinstellungen. Die aktualisierten Einstellungen treten für alle Benutzer, die der Rolle zugewiesen sind, in Kraft.

- Um einem Benutzer die Durchführung einer Aufgabe zu gestatten, weist der Systemadministrator dem Benutzer die Rolle zu.
- Um einen Benutzer von der Durchführung einer Aufgabe abzuhalten, hebt der Systemadministrator die Zuweisung der Rolle zum Benutzer wieder auf.

Die Verwaltung des Zugriffs, der Rollen und Berechtigungen für jeden Benutzer basiert auf dem jeweiligen Benutzeranmeldungskonto. Jedem Benutzer können verschiedene Rollen und Berechtigungen zugewiesen werden.

Benutzern, die bestimmte Objekte nicht sehen bzw. nicht darauf zugreifen können, oder die bestimmte Operationen nicht durchführen können, wurden die entsprechenden Berechtigungen dafür nicht zugewiesen.

Rollenbasierte Zugriffssteuerung

Mit der rollenbasierten Zugriffssteuerung können Systemadministratoren den Benutzerzugriff auf vRealize Log Insight sowie Aufgaben steuern, die Benutzer nach erfolgreicher Anmeldung durchführen können. Um die rollenbasierte Zugriffssteuerung zu implementieren, ordnen Systemadministratoren Berechtigungen und Rollen mit oder aus Benutzeranmeldekonto zu oder heben diese auf.

Benutzer Systemadministratoren können den Zugriff und die Aktionen aller Benutzer steuern, indem sie für das Anmeldekonto des Benutzers Berechtigungen und Rollen gewähren oder diese aufheben.

Berechtigungen Mit Berechtigungen werden die zulässigen Aktionen in vRealize Log Insight gesteuert. Berechtigungen werden auf bestimmte Verwaltungs- oder Benutzeraufgaben in vRealize Log Insight angewendet. Beispiel: Sie können die Berechtigung **Admin anzeigen** gewähren, um einem Benutzer zu erlauben, auf die administrativen vRealize Log Insight-Einstellungen zuzugreifen.

Datensätze	Datensätze bestehen aus einer Gruppe von Filtern. Sie können Datensätze verwenden, um Benutzern Zugriff auf bestimmten Inhalt zu ermöglichen, indem ein Datensatz mit einer Rolle verknüpft wird.
Rollen	Rollen sind Sammlungen aus Berechtigungen und Datensätzen, die mit Benutzern verbunden werden können. Mit Rollen können alle für eine auszuführende Aufgabe erforderlichen Berechtigungen auf bequeme Weise gebündelt werden. Ein Benutzer kann mehreren Rollen zugewiesen werden.

Erstellen eines neuen Benutzerkontos in vRealize Log Insight


Benutzer, denen die Rolle „Super-Admin“ zugewiesen wird, können Benutzerkonten anlegen, um so den Zugang zur vRealize Log Insight-Web-Benutzeroberfläche zu gewähren.

Voraussetzungen

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.

Stellen Sie sicher, dass die Unterstützung für VMware Identity Manager oder Active Directory konfiguriert ist, wenn Sie Benutzerkonten erstellen, die einen dieser Authentifizierungstypen verwenden. Siehe [Aktivieren der Benutzerauthentifizierung über VMware Identity Manager](#) und [Aktivieren der Benutzerauthentifizierung über Active Directory](#)

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Access Control**.
- 3 Klicken Sie auf **Benutzer und Gruppen**.
- 4 Click **New User**.
- 5 Wählen Sie eine Option aus dem Dropdown-Menü **Authentifizierung** aus.
 - Geben Sie, wenn Sie die integrierte Standardauthentifizierung verwenden, einen Benutzernamen, ein Kennwort und optional eine E-Mail-Adresse ein. Kopieren Sie das Kennwort aus dem Textfeld **Kennwort** und stellen Sie es dem Benutzer zur Verfügung.
 - Geben Sie, wenn Sie die Active Directory- oder VMware Identity Manager-Authentifizierung verwenden, die Domäne ein, zu der der Benutzer gehört, einen Benutzernamen und optional die E-Mail-Adresse für das Benutzernamenskonto.

- 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 Klicken Sie auf **Speichern**.

- Für die integrierte Authentifizierung werden die Informationen lokal gespeichert.
- Für die VMware Identity Manager-Authentifizierung überprüft vRealize Log Insight, ob VMware Identity Manager mit der angegebenen Gruppe und deren Domäne synchronisiert ist. Wenn die Gruppe nicht gefunden wird, wird Ihnen ein Dialogfeld eingeblendet, in dem Sie darüber informiert werden, dass vRealize Log Insight diese Gruppe nicht verifizieren kann. Sie können die Gruppe ohne Verifizierung speichern oder den Vorgang abbrechen und den Gruppennamen oder die Domäne korrigieren.

Konfigurieren des VMware Identity Manager -Zugriffs auf Active Directory-Gruppen für vRealize Log Insight

Sie können Active Directory-Gruppen mit vRealize Log Insight über die VMware Identity Manager-Single Sign-On-Authentifizierung verwenden. Ihre Site muss für eine VMware Identity Manager-Authentifizierung mit aktivierter Active Directory-Unterstützung konfiguriert sein. Zudem muss eine Serversynchronisierung eingerichtet sein.

Sie müssen auch Gruppeninformationen in vRealize Log Insight importieren.


Ein VMware Identity Manager-Benutzer übernimmt Rollen, die einer Gruppe zugewiesen sind, der er angehört, sowie die diesem Einzelbenutzer zugewiesenen Rollen. So kann ein Administrator z. B. GruppeA der Rolle **Admin anzeigen** und Benutzer Bob der Rolle **Benutzer** zuweisen. Bob kann außerdem GruppeA zugewiesen werden. Wenn Bob sich anmeldet, übernimmt er die Gruppenrolle und erhält die Berechtigungen für beide Rollen **Admin anzeigen** und **Benutzer**.

Bei dieser Gruppe handelt es sich nicht um eine lokale VMware Identity Manager-Gruppe, sondern um eine Active Directory-Gruppe, die mit VMware Identity Manager synchronisiert ist.

Voraussetzungen

- Stellen Sie sicher, dass Sie das UPN-Attribut (userPrincipalName- bzw. Benutzerprinzipalnamensattribut) konfiguriert haben. Es kann über die Verwaltungsschnittstelle von VMware Identity Manager unter **Identitäts- und Zugriffsmanagement > Benutzerattribute** konfiguriert werden.
- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insight als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei `log-insight-host` die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.
- Stellen Sie sicher, dass Sie die VMware Identity Manager-Unterstützung in vRealize Log Insight konfiguriert haben. Siehe [Aktivieren der Benutzerauthentifizierung über VMware Identity Manager](#).

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Access Control**.
- 3 Click **Users and Groups**.
- 4 Blättern Sie zur Tabelle „Directory Groups“ und klicken Sie auf **Neue Gruppe**.
- 5 Wählen **VMware Identity Manager** aus dem Dropdown-Menü **Typ** aus.
Der von Ihnen bei der Konfiguration der VMware Identity Manager-Unterstützung angegebene Standarddomänenname wird im Textfeld **Domäne** angezeigt.
- 6 Ändern Sie den Domänennamen in den Active Directory-Namen für die Gruppe.
- 7 Geben Sie den Namen der Gruppe ein, die Sie hinzufügen möchten.
- 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 Klicken Sie auf **Speichern**.

vRealize Log Insight überprüft, ob VMware Identity Manager mit der angegebenen Gruppe und deren Domäne synchronisiert ist. Wenn die Gruppe nicht gefunden wird, wird Ihnen ein Dialogfeld eingeblendet, in dem Sie darüber informiert werden, dass vRealize Log Insight diese Gruppe nicht verifizieren kann. Sie können die Gruppe ohne Verifizierung speichern oder den Vorgang abbrechen und den Gruppennamen oder die Domäne korrigieren.

Benutzer, die zu der Gruppe gehören, die Sie hinzugefügt haben, können sich über ihr VMware Identity Manager-Konto bei vRealize Log Insight anmelden. Sie verfügen dann über dieselbe Berechtigungsstufe wie die Gruppe, der sie angehören.

Importieren einer Active Directory-Gruppe in vRealize Log Insight

Anstatt einzelne Domänenbenutzer hinzuzufügen, können Sie Domänengruppen hinzufügen, um den Benutzern die Anmeldung bei vRealize Log Insight zu gestatten.

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.


Die Active Directory-Gruppen, die Sie vRealize Log Insight hinzufügen, müssen entweder der Domäne des Bindungsbenutzers oder einer Domäne, der die Domäne des Bindungsbenutzers vertraut, angehören.

Ein Active Directory-Benutzer übernimmt Rollen, die einer Gruppe zugewiesen sind, der er angehört, sowie die diesem Einzelbenutzer zugewiesenen Rollen. So kann ein Administrator z. B. GruppeA der Rolle **Admin anzeigen** und Benutzer Bob der Rolle **Benutzer** zuweisen. Bob kann außerdem GruppeA zugewiesen werden. Wenn Bob sich anmeldet, übernimmt er die Gruppenrolle und erhält die Berechtigungen für beide Rollen **Admin anzeigen** und **Benutzer**.

Voraussetzungen

- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insight als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei `log-insight-host` die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.
- Vergewissern Sie sich, dass die AD-Unterstützung konfiguriert ist. Siehe [Aktivieren der Benutzerauthentifizierung über Active Directory](#).

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Access Control**.
- 3 Click **Users and Groups**.
- 4 Klicken Sie unter „Directory-Gruppen“ auf **Neue Gruppe**.

- 5 Klicken Sie im Dropdown-Menü **Typ** auf „Active Directory“.

Der von Ihnen bei der Konfiguration der Active Directory-Unterstützung angegebene Standarddomänenname wird im Textfeld **Domäne** angezeigt. Wenn Sie Gruppen zur Standarddomäne hinzufügen, dürfen Sie den Domänennamen nicht ändern.

- 6 (Optional) Wenn Sie eine Gruppe aus einer Domäne, die der Standarddomäne vertraut, hinzufügen möchten, geben Sie den Namen der vertrauenden Domäne in das Textfeld **Domäne** ein.
- 7 Geben Sie den Namen der Gruppe ein, die Sie hinzufügen möchten.
- 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 Klicken Sie auf **Speichern**.

vRealize Log Insight verifiziert, ob die AD-Gruppe in der Domäne, die Sie angegeben haben, oder in einer vertrauenswürdigen Domäne vorhanden ist. Wenn die Gruppe nicht gefunden wird, wird Ihnen ein Dialogfeld eingeblendet, in dem Sie darüber informiert werden, dass vRealize Log Insight diese Gruppe nicht verifizieren kann. Sie können die Gruppe ohne Verifizierung speichern oder den Vorgang abbrechen und den Gruppennamen korrigieren.

Benutzer, die zu der Active Directory-Gruppe gehören, die Sie hinzugefügt haben, können sich über ihr Domänenkonto bei vRealize Log Insight anmelden. Sie verfügen dann über dieselbe Berechtigungsstufe wie die Gruppe, der sie angehören.

Authentifizieren von Benutzern mit domänenübergreifender Gruppen-Mitgliedschaft

Es gibt zwei Möglichkeiten, wie Administratoren Benutzern aus einer anderen vertrauenswürdigen Domäne eine Authentifizierung für vRealize Log Insight ermöglichen können.

- Sie können jeden Benutzer manuell hinzufügen.
- Sie können eine Gruppe in der Domäne der Benutzer konfigurieren und die Gruppe hinzufügen.

Definieren eines Datensatzes


Sie können einen Datensatz definieren, um Benutzerzugriff auf bestimmte Inhalte zu gewährleisten.

Textbasierte Einschränkungen werden für Datensätze nicht unterstützt.

Voraussetzungen

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.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Access Control**.
- 3 Click **Data Sets**.
- 4 Klicken Sie auf **Neuer Datensatz**.
- 5 Klicken Sie auf **Filter hinzufügen**.
- 6 Verwenden Sie das erste Dropdown-Menü, um ein beliebiges innerhalb von vRealize Log Insight definiertes Feld zu verwenden.

Beispiel: **hostname**.

Die Liste enthält alle definierten Felder, die statisch verfügbar sind, Inhaltspaketen und in benutzerdefiniertem Inhalt.

Hinweis Numerische Felder enthalten zusätzliche Operatoren, die in Zeichenfolgenfeldern nicht vorkommen: **=**, **>**, **<**, **>=** und **<=**. Diese Operatoren führen numerische Vergleiche aus. Durch ihre Verwendung können andere Ergebnisse als bei der Verwendung von Zeichenfolgenoperatoren erzielt werden. Beispiel: Der Filter **response_time = 02** ergibt als Treffer ein Ereignis, das ein Feld **response_time** mit einem Wert von 2 enthält. Der Filter **response_time enthält 02** ergibt nicht denselben Treffer.

- 7 Verwenden Sie das zweite Dropdown-Menü, um den Vorgang auszuwählen, der auf das im ersten Dropdown-Menü ausgewählte Feld angewendet werden soll.

Wählen Sie zum Beispiel **enthält**. Der Filter **enthält** gleicht vollständige Token ab: Wenn Sie z. B. den Suchbegriff „err“ eingeben, werden keine Übereinstimmungen mit `error` ausgegeben.

- 8 Geben Sie im Textfeld rechts neben dem Dropdown-Menü für den Filter den Wert ein, den Sie als Filter verwenden möchten.

Sie können mehrere Werte verwenden. Der Operator zwischen diesen Werten ist **ODER**.

Hinweis Das Textfeld ist nicht verfügbar, wenn Sie im zweiten Dropdown-Menü den Operator **ist vorhanden** auswählen.

9 (Optional) Klicken Sie auf **Filter hinzufügen**, um weitere Filter hinzuzufügen.

10 Click **Save**.

Weiter

Ordnen Sie einer Benutzerrolle einen Datensatz zu. Weitere Informationen hierzu finden Sie unter [Erstellen und Ändern von Rollen](#).


Erstellen und Ändern von Rollen

Sie können benutzerdefinierte Rollen erstellen oder vordefinierte Rollen ändern, um den Benutzern die Durchführung bestimmter Aufgaben sowie den Zugriff auf bestimmte Inhalte zu gestatten.

Voraussetzungen

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.

Vorgehensweise

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

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

3 Click **Roles**.

4 Klicken Sie auf **Neue Rolle** oder auf , um eine vorhandene Rolle zu bearbeiten.

Sie müssen zunächst die Rollen „Super Admin“ und „Benutzer“ klonen, bevor Sie sie bearbeiten können.

5 Ändern Sie die Textfelder **Name** und **Beschreibung**.

6 Wählen Sie eine oder mehrere Berechtigung(en) aus der Liste „Berechtigungen“ aus.

Option	Beschreibung
Admin bearbeiten	Damit können Admin-Informationen und -Einstellungen bearbeitet werden
Admin anzeigen	Damit können Admin-Informationen und -Einstellungen angezeigt werden
Freigegebene bearbeiten	Damit können freigegebene Inhalte bearbeitet werden
Analytics	Damit kann die Interaktive Analyse verwendet werden
Dashboard	Damit können Dashboards angezeigt werden

7 (Optional) Wählen Sie rechts aus der Liste **Datensätze** einen Datensatz aus, welcher der Benutzerrolle zugewiesen werden soll.

8 Click **Save**.



Löschen eines Benutzerkontos aus vRealize Log Insight

Benutzerkonten können über die Benutzeroberfläche für Administratoren von vRealize Log Insight gelöscht werden.

Voraussetzungen

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.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Access Control**.
- 3 Click **Users and Groups**.
- 4 Aktivieren Sie das Kontrollkästchen neben dem Benutzernamen, der gelöscht werden soll.
- 5 Klicken Sie auf das Symbol **Löschen** .

Konfigurieren der Authentifizierung

3

Sie können mehrere Authentifizierungsmethoden für Ihre Bereitstellung verwenden.

Die folgenden Authentifizierungsmethoden stehen zur Verfügung: Lokale Authentifizierung, VMware Identity Manager-Authentifizierung und Active Directory-Authentifizierung. Sie können in einer Bereitstellung mehr als eine Methode verwenden. Die Benutzer wählen bei der Anmeldung dann einen Authentifizierungstyp aus.

vRealize Log Insight umfasst eine Version von vRealize Log Insight, die auf der Seite für den Produktdownload zur Verfügung steht. Die folgenden Funktionen sind enthalten:

- Verzeichnisintegration, um Benutzer anhand von vorhandenen Verzeichnissen wie Active Directory oder LDAP zu authentifizieren.
- Single Sign-On-Integration mit anderen VMware-Produkten, die die Single Sign-On-Funktion auch unterstützen.
- Single Sign-On mit verschiedenen Drittanbieter-Identitätsanbietern wie ADFS, Ping Federate und anderen.
- Zweistufige Authentifizierung durch Integration mit Drittanbietersoftware wie RSA SecurID, Entrust und anderen. Die zweistufige Authentifizierung mit VMware Verify ist nicht enthalten.

Die lokale Authentifizierung ist eine Komponente von vRealize Log Insight. Um diese anwenden zu können, müssen Sie einen lokalen Benutzer erstellen und ein Kennwort festlegen, das auf dem vRealize Log Insight-Server gespeichert wird. vRealize Log Insight und Active Directory müssen von einem Produktadministrator aktiviert worden sein.

Dieses Kapitel behandelt die folgenden Themen:

- [Aktivieren der Benutzerauthentifizierung über VMware Identity Manager](#)
- [Aktivieren der Benutzerauthentifizierung über Active Directory](#)

Aktivieren der Benutzerauthentifizierung über VMware Identity Manager

Die VMware Identity Manager-Authentifizierung kann mit vRealize Log Insight verwendet werden, wenn diese vom Administrator aktiviert wurde.


Mit der VMware Identity Manager-Authentifizierung haben Benutzer die Möglichkeit, eine Single-Sign-On-Anmeldung für alle VMware-Produkte vorzunehmen, die den gleichen Identity Manager verwenden.

Active Directory-Benutzer können sich ebenfalls mit VMware Identity Manager authentifizieren, wenn die Active Directory- und VMware Identity Manager-Server synchronisiert sind. Weitere Informationen zur Synchronisierung erhalten Sie in der VMware Identity Manager-Dokumentation.

Voraussetzungen

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.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Klicken Sie unter „Konfiguration“ auf **Authentifizierung**.
- 3 Wählen Sie **Single Sign-On aktivieren** aus.
- 4 Geben Sie in das Textfeld **Host** einen Hostbezeichner für die VMware Identity Manager-Instanz ein, die für die Authentifizierung von Benutzern verwendet werden soll.

Beispiel: **company-name.vmwareidentity.com**.

- 5 Geben Sie im Textfeld **API-Port** den Port an, der für die Herstellung einer Verbindung mit der VMware Identity Manager-Instanz verwendet werden soll. Die Standardeinstellung ist 443.
- 6 Optional geben Sie den VMware Identity Manager-Mandanten ein. Dies ist nur erforderlich, wenn der Mandantenmodus in VMware Identity Manager als „Mandant in Pfad“ konfiguriert ist.
- 7 Geben Sie in die Textfelder **Benutzername** und **Kennwort** die Benutzeranmeldedaten für VMware Identity Manager ein.

Diese Informationen werden nur einmal bei der Konfiguration beim Erstellen eines vRealize Log Insight-Clients in VMware Identity Manager verwendet und nicht lokal in vRealize Log Insight gespeichert. Der Benutzer muss über die Berechtigung zur Ausführung von API-Befehlen für den Mandanten verfügen.

- 8 Klicken Sie auf **Verbindung testen**, um zu überprüfen, ob die Verbindung funktioniert.
- 9 Wählen Sie im Dropdown-Menü **Host für Umleitungs-URL** den Hostnamen oder die IP-Adresse aus, der bzw. die in der Umleitungs-URL für die Registrierung bei VMware Identity Manager verwendet werden soll.

Wenn mindestens eine virtuelle IP-Adresse (VIP) für den integrierten Lastausgleichsdienst definiert ist, leitet VMware Identity Manager zur ausgewählten VIP um. Wenn der integrierte Lastausgleichsdienst nicht definiert ist, wird stattdessen die IP-Adresse des Master-Knotens verwendet.

- 10 Wählen Sie aus, ob für Active Directory-Benutzer die Anmeldung über VMware Identity Manager zulässig ist.

Diese Option kann für Active Directory-Benutzer verwendet werden, wenn VMware Identity Manager mit der betreffenden Active Directory-Instanz synchronisiert ist.

- 11 Click **Save**.


Aktivieren der Benutzerauthentifizierung über Active Directory

Sie können Benutzer über Active Directory authentifizieren. Dies vereinfacht den Anmeldevorgang für Benutzer, da sie ein allgemeines Kennwort für mehrere Zwecke verwenden können.

Voraussetzungen

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.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Klicken Sie unter „Konfiguration“ auf **Authentifizierung**.
- 3 Wählen Sie **AD-Unterstützung aktivieren**.
- 4 Geben Sie im Textfeld **Standarddomäne** einen Domänennamen ein.

Beispiel: **firmenname.com**.

Hinweis Im Standarddomänen-Textfeld darf nicht mehr als eine Domäne eingegeben werden. Wird der Standarddomäne, die Sie angegeben haben, von anderen Domänen vertraut, verwendet vRealize Log Insight die Standarddomäne und den Bindungsbenutzer, um AD-Benutzer und -Gruppen in den vertrauenden Domänen zu überprüfen.

Beim Wechsel zu einer anderen Domäne, die bereits Benutzer und Gruppen enthält, schlägt die Authentifizierung für die vorhandenen Benutzer und Gruppen fehl, und von den vorhandenen Benutzern gespeicherte Daten gehen verloren.

- 5 Im Falle von Domänencontrollern mit Standortinformationen oder Sicherheitsbeschränkungen geben Sie die Domänencontroller, die dieser vRealize Log Insight-Instanz am nächsten sind, manuell an.

Hinweis Active Directory-Autorisierungsserver mit Lastausgleich werden nicht unterstützt.

- 6 Geben Sie die Anmeldedaten eines der Standarddomäne angehörenden Bindungsbenutzers ein.
vRealize Log Insight verwendet die Standarddomäne und den Bindungsbenutzer, um AD-Benutzer und -Gruppen in der Standarddomäne und in Domänen, die der Standarddomäne vertrauen, zu überprüfen.
- 7 Geben Sie die Werte für den Verbindungstyp an.
Diese Verbindung wird für die Active Directory-Authentifizierung verwendet.
- 8 Click **Save**.

Weiter

Erteilen Sie AD-Benutzern und -Gruppen Berechtigungen, um auf die aktuelle Instanz von vRealize Log Insight zuzugreifen.

Konfigurieren des für Active Directory zu verwendenden Protokolls

Sie können das Protokoll konfigurieren, das beim Verbinden mit Active Directory verwendet werden soll. Wenn sich vRealize Log Insight mit einem Active Directory verbindet, wird standardmäßig zunächst versucht, eine SSL-LDAP-Verbindung und dann, falls erforderlich, eine Nicht-SSL-LDAP-Verbindung herzustellen.

Wenn Sie die Active Directory-Kommunikation auf ein bestimmtes Protokoll beschränken oder die Reihenfolge der für die Verbindungsversuche zu verwendenden Protokolle ändern möchten, müssen Sie zusätzliche Konfigurationen in der virtuellen vRealize Log Insight-Appliance vornehmen.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die Root-Benutzer-Anmeldedaten verfügen, um sich bei der virtuellen vRealize Log Insight-Appliance anzumelden. Siehe [SSH-Root-Kennwort für die virtuelle vRealize Log Insight-Appliance konfigurieren](#).
- Um SSH-Verbindungen zu aktivieren, überprüfen Sie zunächst, ob der TCP-Port 22 geöffnet ist.

Vorgehensweise

- 1 Stellen Sie eine SSH-Verbindung zur virtuellen vRealize Log Insight-Appliance her und melden Sie sich als Root-Benutzer an.
- 2 Navigieren Sie zum folgenden Speicherort: `/storage/var/loginsight/config`
- 3 Suchen Sie die neueste Konfigurationsdatei mit der höchsten [Ziffer]: `/storage/core/loginsight/config/loginsight-config.xml#[number]`
- 4 Kopieren Sie die neueste Konfigurationsdatei: `/storage/core/loginsight/config/loginsight-config.xml#[number]`
- 5 Erhöhen Sie die [Ziffer] und speichern Sie die Datei am folgenden Speicherort: `/storage/core/loginsight/config/loginsight-config.xml#[number + 1]`
- 6 Öffnen Sie die Datei zum Bearbeiten.
- 7 Fügen Sie im Abschnitt Authentication die Zeile hinzu, die der Konfiguration entspricht, die Sie anwenden möchten:

Option	Beschreibung
<code><ad-protocols value="LDAP" /></code>	Speziell, um LDAP ohne SSL zu verwenden
<code><ad-protocols value="LDAPS" /></code>	Speziell für die ausschließliche Verwendung von LDAP mit SSL

Option	Beschreibung
<code><ad-protocols value="LDAP,LDAPS" /></code>	Speziell, um erst LDAP und dann LDAP mit SSL zu verwenden
<code><ad-protocols value="LDAPS,LDAP" /></code>	Speziell, um erst LDAPS und dann LDAP ohne SSL zu verwenden

Wenn Sie kein Protokoll auswählen, versucht vRealize Log Insight zunächst LDAP und dann LDAP mit SSL zu verwenden.

- 8 Speichern und schließen Sie die Datei.
- 9 Führen Sie den Befehl `service loginsight restart` aus.

Konfigurieren von vRealize Log Insight

4

Sie können vRealize Log Insight konfigurieren und anpassen, um Standardeinstellungen, Netzwerkeinstellungen und Speicherressourcen zu ändern. Sie können außerdem Systembenachrichtigungen konfigurieren.

Dieses Kapitel behandelt die folgenden Themen:

- [vRealize Log Insight Grenzwerte für die Konfiguration](#)
- [Konfigurieren der Einstellungen für die virtuelle Appliance](#)
- [Zuweisen einer permanenten Lizenz zu vRealize Log Insight](#)
- [Protokollspeicherrichtlinie](#)
- [Verwalten von Systembenachrichtigungen](#)
- [Hinzufügen eines Ziels für die vRealize Log Insight-Ereignisweiterleitung](#)
- [Synchronisieren der Uhrzeit der virtuellen vRealize Log Insight-Appliance](#)
- [Konfigurieren des SMTP-Servers für vRealize Log Insight](#)
- [Installieren eines benutzerdefinierten SSL-Zertifikats](#)
- [Ändern des Standard-Zeitlimits für vRealize Log Insight-Websitzungen](#)
- [Archive](#)
- [Neustart des vRealize Log Insight-Diensts](#)
- [Ausschalten der virtuellen vRealize Log Insight-Appliance](#)
- [Herunterladen eines Support-Pakets für vRealize Log Insight](#)
- [Teilnahme am VMware-Programm zur Verbesserung der Benutzerfreundlichkeit oder Verlassen des Programms](#)

vRealize Log Insight Grenzwerte für die Konfiguration

Wenn Sie vRealize Log Insight konfigurieren, müssen Sie die Grenzwerte einhalten.

Tabelle 4-1. vRealize Log Insight Maximalwerte für die Konfiguration

Element	Maximalwert
Knoten-Konfiguration	
CPU	16 vCPUs
Arbeitsspeicher	32 GB
Speichergerät (VMDK)	2 TB - 512 Byte
Gesamter adressierbarer Speicher	4 TB (+ Betriebssystemlaufwerk) Maximal 4 TB adressierbarer Protokollspeicher auf VMDKs mit einer maximalen Speichergröße von 2 TB pro Gerät. Dabei können zwei 2 TB-Geräte, vier 1 TB-Geräte usw. verwendet werden. Wird die maximale Speichergröße erreicht, muss mit einer größeren Clustergröße gearbeitet werden, anstatt bestehenden virtuellen Maschinen weitere Festplatten hinzuzufügen.
Syslog-Verbindungen	750
Clusterkonfiguration	
Knoten	12 (Master + 11 Worker)
Aufnahme pro Knoten	
Ereignisse pro Sekunde	15.000 eps
Syslog-Nachrichtenlänge	10 KB (Textfeld)
Ingestion-API HTTP-POST-Anforderung	16 KB (Textfeld); 4 MB pro HTTP POST-Anforderung
Integrationen	
vRealize Operations Manager	1
vSphere vCenter Server	10
Active Directory-Domäne	1
E-Mail-Server	1
DNS-Server	2
NTP-Server	4
Ereignisweiterleitungen	10

Konfigurieren der Einstellungen für die virtuelle Appliance

Sie können die Einstellungen der virtuellen Appliance, einschließlich Speicherkapazität und Arbeitsspeicher bzw. CPU-Kapazität, ändern.

SSH-Root-Kennwort für die virtuelle vRealize Log Insight - Appliance konfigurieren

Die SSH-Verbindung zur virtuellen Appliance ist standardmäßig deaktiviert. Sie können das SSH-Root-Kennwort über die VMware Remote Console konfigurieren oder die Konfiguration bei der Bereitstellung der virtuellen vRealize Log Insight-Appliance vornehmen.

Als Best Practice wird das Festlegen des SSH-Root-Kennworts während der Bereitstellung der .ova-Datei von vRealize Log Insight empfohlen. Weitere Informationen finden Sie unter [Bereitstellen der virtuellen vRealize Log Insight-Appliance](#).

Sie können auch SSH aktivieren und das Root-Kennwort über die VMware Remote Console festlegen.

Voraussetzungen

Stellen Sie sicher, dass die virtuelle vRealize Log Insight-Appliance bereitgestellt ist und ordnungsgemäß ausgeführt wird.

Vorgehensweise

- 1 Klicken Sie in der vSphere-Client-Bestandsliste auf die virtuelle vRealize Log Insight-Appliance und öffnen Sie die Registerkarte **Konsole**.
- 2 Rufen Sie mit der im Startbild angegebenen Tastenkombination eine Befehlszeile auf.
- 3 Geben Sie in der Konsole **root** ein und drücken Sie die Eingabetaste. Lassen Sie das Kennwort leer und drücken Sie die Eingabetaste.

In der Konsole wird folgende Meldung angezeigt: Kennwortänderung angefordert. Wählen Sie ein neues Kennwort.

- 4 Lassen Sie das alte Kennwort leer und drücken Sie die Eingabetaste.
- 5 Geben Sie ein neues Kennwort für den Root-Benutzer ein, drücken Sie die Eingabetaste, geben Sie das neue Kennwort für den Root-Benutzer erneut ein und drücken Sie die Eingabetaste.

Das Kennwort muss aus mindestens acht Zeichen bestehen und mindestens einen Großbuchstaben, einen Kleinbuchstaben, eine Ziffer und ein Sonderzeichen enthalten. Sie können dasselbe Zeichen nicht mehr als vier Mal wiederholen.

Es wird folgende Meldung angezeigt: Kennwort geändert.

Weiter

Sie können das Root-Kennwort verwenden, um SSH-Verbindungen zur virtuellen vRealize Log Insight-Appliance herzustellen.

Ändern der Netzwerkeinstellungen der vApp für vRealize Log Insight

Sie können die Netzwerkeinstellungen der virtuellen Appliance für vRealize Log Insight ändern, indem Sie die vApp-Eigenschaften in vSphere Client bearbeiten.

Voraussetzungen

Stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen zum Bearbeiten von vApp-Eigenschaften verfügen.

Vorgehensweise

- 1 Schalten Sie die vRealize Log Insight-vApp aus.
- 2 Klicken Sie mit der rechten Maustaste auf die vRealize Log Insight-vApp in der Bestandsliste und klicken Sie auf **Einstellungen bearbeiten**.
- 3 Klicken Sie auf die Registerkarte **Optionen** und wählen Sie **vApp-Optionen > IP-Zuteilungsrichtlinie**.
- 4 Wählen Sie eine Zuteilungsoption für IP-Adressen.

Option	Beschreibung
Fest	IP-Adressen werden manuell konfiguriert. Es wird keine automatische Zuteilung vorgenommen.
Vorübergehend	IP-Adressen werden beim Einschalten der vApp automatisch mithilfe von IP-Pools aus einem angegebenen Bereich zugeteilt. Die IP-Adressen werden freigegeben, wenn die Appliance ausgeschaltet wird.
DHCP	Zum Zuteilen der IP-Adressen wird ein DHCP-Server verwendet. Die vom DHCP-Server zugewiesenen Adressen sind in den OVF-Umgebungen von virtuellen Maschinen sichtbar, die in der vApp gestartet wurden.

- 5 (Optional) Wenn Sie **Fest** auswählen, klicken Sie auf **vApp-Optionen > Eigenschaften** und weisen Sie der vApp für vRealize Log Insight eine IP-Adresse, eine Netzmaske, einen DNS und einen Hostnamen zu.

Vorsicht Geben Sie nicht mehr als zwei Domännennamenserver an. Wenn Sie mehr als zwei Domännennamenserver angeben, werden alle konfigurierten Domännennamenserver in der virtuellen vRealize Log Insight-Appliance ignoriert.

- 6 Schalten Sie die vApp für vRealize Log Insight ein.

Erhöhen der Speicherkapazität der virtuellen vRealize Log Insight -Appliance

Sie können die Speicherressourcen, die vRealize Log Insight zugewiesen sind, erhöhen, wenn Ihre Nachfrage wächst.

Vergrößern Sie den Speicherplatz, indem Sie der virtuellen Appliance vRealize Log Insight eine neue virtuelle Festplatte hinzufügen. Sie können bis zu einem gesamten adressierbaren Speicher von 4 TB (+ Speicherplatz für das Betriebssystem) so viele Festplatten hinzufügen wie Sie möchten. Der gesamte Speicher kann aus einer Kombination von zwei 2-TB-Festplatten oder vier 1-TB-Festplatten, usw. bestehen. Weitere Informationen hierzu finden Sie unter [vRealize Log Insight Grenzwerte für die Konfiguration](#).

Voraussetzungen

- Log in to the vSphere Client as a user who has privileges to modify the hardware of virtual machines in the environment.
- Fahren Sie die virtuelle vRealize Log Insight-Appliance sicher herunter. Siehe [Ausschalten der virtuellen vRealize Log Insight-Appliance](#).

Vorgehensweise

- 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 Wählen Sie **Festplatte**, und klicken Sie auf **Weiter**.

4 Wählen Sie **Neue virtuelle Festplatte erstellen**, und klicken Sie auf **Weiter**.

a Geben Sie die Festplattenkapazität ein.

vRealize Log Insight unterstützt virtuelle Festplatten von bis zu 2 TB. Wenn Sie mehr Kapazität benötigen, fügen Sie mehr als eine virtuelle Festplatte hinzu.

b Auswählen eines Festplattenformats.

Option	Beschreibung
Thick-Provision Lazy-Zeroed	Erstellt eine virtuelle Festplatte im Thick-Standardformat. Der für die virtuelle Festplatte erforderliche Speicherplatz wird bei Erstellung der virtuellen Festplatte zugewiesen. Die Daten, die auf dem physischen Gerät vorhanden sind, werden nicht während des Anlegens, sondern später während der ersten Schreibvorgänge der virtuellen Appliance gelöscht.
Thick-Provision Eager-Zeroed	Erstellt einen Typ einer virtuellen Festplatte im Thick-Format, der Clusterfunktionen, wie z. B. Fault Tolerance, unterstützt. Der Speicher, den die virtuelle Festplatte benötigt, wird beim Erstellen zugewiesen. Im Gegensatz zum Flat-Format werden die auf dem physischen Gerät verbleibenden Daten durch Nullbyte ersetzt („zeroed out“), wenn die virtuelle Festplatte erstellt wird. Das Anlegen von Festplatten in diesem Format kann wesentlich länger dauern als das Anlegen anderer Festplattentypen. Erstellen Sie, soweit möglich, die virtuelle vRealize Log Insight-Appliance mit Festplatten vom Typ Thick-Provisioned, Eager-Zeroed, um Leistung und Betrieb der virtuellen Appliance zu optimieren.
Thin Provision	Erstellt eine Festplatte im Thin-Format. Verwenden Sie dieses Format, um Speicherplatz zu sparen.

c Zum Auswählen eines Datenspeichers navigieren Sie zum Speicherort des Datenspeichers und klicken auf **Weiter**.

5 Akzeptieren Sie den Standardknoten des virtuellen Geräts und klicken Sie auf **Weiter**.

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

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

Wenn Sie die virtuelle vRealize Log Insight-Appliance hochfahren, erkennt die virtuelle Maschine die neue Festplatte und fügt sie dem Datenvolumen hinzu. Schalten Sie zuerst die virtuelle Maschine vollständig aus. Informationen zum Einschalten von virtuellen Appliances finden Sie unter <https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-6-pubs.html>.

Vorsicht Nachdem Sie eine Festplatte zur virtuellen Appliance hinzugefügt haben, können Sie sie nicht mehr auf sichere Weise entfernen. Das Entfernen von Festplatten von der virtuellen vRealize Log Insight-Appliance kann zu einem vollständigen Datenverlust führen.

Hinzufügen von Arbeitsspeicher und CPU zur virtuellen vRealize Log Insight -Appliance

Sie können die Arbeitsspeichermenge und die Anzahl der CPUs ändern, die einer virtuellen vRealize Log Insight-Appliance nach der Bereitstellung zugeteilt werden.

Sie müssen möglicherweise die Ressourcenzuweisung anpassen, beispielsweise wenn die Anzahl von Ereignissen in Ihrer Umgebung zunimmt.

Voraussetzungen

- Melden Sie sich bei vSphere Client als Benutzer mit Berechtigungen zum Ändern der Hardware der virtuellen Maschinen in Ihrer Umgebung an.
- Fahren Sie die virtuelle vRealize Log Insight-Appliance sicher herunter. Siehe [Ausschalten der virtuellen vRealize Log Insight-Appliance](#).

Vorgehensweise

- 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 Passen Sie die CPU- und Arbeitsspeichermenge nach Bedarf an.
- 4 Review the information and click **Finish**.
- 5 Click **OK** to save your changes and close the dialog box.

Wenn Sie die virtuelle vRealize Log Insight-Appliance einschalten, beginnt die virtuelle Maschine mit der Nutzung der neuen Ressourcen.

Zuweisen einer permanenten Lizenz zu vRealize Log Insight

Sie können vRealize Log Insight nur mit einem gültigen Lizenzschlüssel nutzen.

Wenn Sie vRealize Log Insight von der VMware-Website herunterladen, erhalten Sie eine Testlizenz. Diese Lizenz ist 60 Tage lang gültig. Nach Ablauf der Testlizenz müssen Sie eine permanente Lizenz erwerben, um vRealize Log Insight weiter nutzen zu können.

Zur Gewährleistung der Lösungsinteroperabilität können Benutzer der VMware NSX-Editionen Standard, Advanced oder Enterprise VMware vRealize® Log Insight mit ihrem NSX-Lizenzschlüssel lizenzieren. Weitere Informationen dazu finden Sie in der VMware NSX-Dokumentation.


Im Verwaltungsabschnitt der Web-Benutzeroberfläche von vRealize Log Insight können Sie den vRealize Log Insight-Lizenzierungsstatus überprüfen und Ihre Lizenz verwalten.

Voraussetzungen

- Beziehen Sie über My VMware™ einen gültigen Lizenzschlüssel.

- 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.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Wählen Sie unter „Management“ **Lizenz**.
- 3 Geben Sie im Textfeld **Lizenzschlüssel** Ihren Lizenzschlüssel ein und klicken Sie auf **Schlüssel festlegen**. Geben Sie hier den VMware NSX-Lizenzschlüssel ein, sofern Sie über einen solchen verfügen.
- 4 Stellen Sie sicher, dass der Lizenzstatus „Aktiv“ ist und dass Lizenztyp und Ablauftag korrekt sind.

Protokollspeicherrichtlinie

Die virtuelle vRealize Log Insight-Appliance benötigt mindestens 100 GB Speicher für eingehende Protokolle.

Wenn das Volumen der in vRealize Log Insight importierten Protokolle die 100-GB-Grenze erreicht, werden alte Protokollmeldungen automatisch und in regelmäßigen Abständen in der Eingangsreihenfolge stillgelegt. Um alte Meldungen aufzubewahren, können Sie die Archivierungsfunktion von vRealize Log Insight aktivieren. Weitere Informationen hierzu finden Sie unter [Aktivieren oder Deaktivieren der Datenarchivierung in vRealize Log Insight](#).

Von vRealize Log Insight gespeicherte Daten sind unveränderbar. Nachdem ein Protokoll importiert wurde, kann dieses erst entfernt werden, wenn es automatisch stillgelegt wird.

Verwalten von Systembenachrichtigungen

vRealize Log Insight bietet integrierte Systembenachrichtigungen zu Aktivitäten mit Bezug zum vRealize Log Insight-Systemzustand, z. B. wenn der Festplattenspeicher fast ausgeschöpft ist oder wenn alte Protokolldateien gelöscht werden sollen. Administratoren können konfigurieren, wie oft und an wen Systembenachrichtigungen gesendet werden.

Systembenachrichtigungen informieren Sie über kritische Probleme, die eine sofortige Behandlung erfordern, stattdessen Sie mit Warnungen aus, die eventuell eine entsprechende Reaktion verlangen, und dokumentieren die reguläre Systemaktivität. Systembenachrichtigungen werden im Verlauf eines Upgrades ausgesetzt, aber sonst durchgehend übermittelt.

Administratoren können festlegen, wie häufig und an welche E-Mail-Adressen Benachrichtigungen nach der Auslösung gesendet werden. Systembenachrichtigungen zu vRealize Log Insight können auch an Drittanbieteranwendungen gesendet werden.

Systembenachrichtigungen unterscheiden sich von Warnungsabfragen, die von Benutzern definiert werden. Weitere Informationen zu Warnungsabfragen finden Sie unter [Hinzufügen einer Warnungsabfrage in Log Insight zum Senden von E-Mail-Benachrichtigungen](#).

vRealize Log Insight-Systembenachrichtigungen

vRealize Log Insight bietet Ihnen zwei Gruppen von Benachrichtigungen: allgemeine Benachrichtigungen, die für alle Produktkonfigurationen gelten, und Benachrichtigungen zu Cluster für Cluster-basierte Bereitstellungen.

Die folgenden Tabellen stellen die Systembenachrichtigungen für vRealize Log Insight und eine entsprechende Beschreibung dar.

Allgemeine Systembenachrichtigungen

vRealize Log Insight sendet Benachrichtigungen, wenn die Bedingungen eventuell ein administratives Eingreifen erfordern, einschließlich Archivierungsfehler oder Verzögerungen bei der Warnungsplanung.

Benachrichtigungsname	Beschreibung
Älteste Daten werden bald nicht mehr durchsuchbar sein	<p>Diese Benachrichtigung informiert Sie, wenn in vRealize Log Insight eine Stilllegung alter Daten aus dem Speicher der virtuellen Appliance bevorsteht, und gibt die bei der aktuellen Aufnahmerate erwartete Menge durchsuchbarer Daten an. Ersetzte Daten werden archiviert, wenn Sie die Archivierung konfiguriert haben, oder andernfalls gelöscht.</p> <p>Die Benachrichtigung wird nach jedem Neustart des vRealize Log Insight-Diensts gesendet.</p>
Repository-Aufbewahrungszeit	<p>Der Aufbewahrungszeitraum ist die Zeitdauer, in der Daten auf der lokalen Festplatte Ihrer vRealize Log Insight-Instanz gespeichert sind. Dieser Zeitraum wird durch den Umfang der Daten, die das System aufnehmen kann, und die aktuelle Datenaufnahmerate bestimmt. Wenn Sie beispielsweise täglich 10 GB Daten (nach der Indizierung) erhalten und über 300 GB Speicherplatz verfügen, beträgt Ihr Aufbewahrungszeitraum 30 Tage. Wenn diese Grenze erreicht ist, werden alte Daten entfernt, um Platz für neu aufgenommene Daten zu schaffen.</p> <p>Diese Benachrichtigung informiert Sie, wenn die Menge der durchsuchbaren Daten, die vRealize Log Insight bei den aktuellen Aufnahmeraten speichern kann, den in der virtuellen Appliance verfügbaren Speicherplatz übersteigt.</p> <p>Admin-Benutzer können den Schwellenwert für Speicherplatzmeldungen festlegen. Weitere Informationen hierzu finden Sie unter Konfigurieren von vRealize Log Insight zum Senden von Benachrichtigungen über den Systemzustand.</p>

Benachrichtigungsname	Beschreibung
Verworfenne Ereignisse	<p>Diese Benachrichtigung informiert Sie darüber, dass vRealize Log Insight nicht alle eingegangenen Protokollmeldungen aufnehmen konnte.</p> <ul style="list-style-type: none"> ■ Im Falle von durch den vRealize Log Insight-Server erkannten Löschungen von TCP-Meldungen wird in beiden Fällen eine Systembenachrichtigung in folgender Weise gesendet: <ul style="list-style-type: none"> ■ Einmal pro Tag ■ Bei jedem manuell oder automatisch ausgeführten Neustart des vRealize Log Insight-Diensts. ■ Die E-Mail enthält die Anzahl der gelöschten Meldungen seit dem Versenden der letzten Benachrichtigungs-E-Mail und die Gesamtzahl der Meldungslöschungen seit dem letzten Neustart von vRealize Log Insight. <p>Hinweis Die in der Zeile „Gesendet“ angegebene Uhrzeit wird durch den E-Mail-Client vorgegeben und ist die Zeit der lokalen Zeitzone, während im E-Mail-Text die UTC-Zeit angegeben wird.</p>
Beschädigter Index-Bucket	<p>Diese Benachrichtigung informiert Sie darüber, dass ein Teil des Festplattenindexes beschädigt ist. Ein korrupter Index weist üblicherweise auf ernsthafte Probleme im zugrunde liegenden Speichersystem hin. Der beschädigte Teil des Indexes wird von der Bedienung von Abfragen ausgeschlossen. Ein korrupter Index hat Auswirkungen auf die Aufnahme neuer Daten. vRealize Log Insight überprüft die Integrität des Indexes beim Start des Diensts. Wenn eine Beschädigung festgestellt wird, sendet vRealize Log Insight eine Systembenachrichtigung in folgender Weise:</p> <ul style="list-style-type: none"> ■ Einmal pro Tag ■ Bei jedem manuell oder automatisch ausgeführten Neustart des vRealize Log Insight-Diensts.

Benachrichtigungsname	Beschreibung
Zu wenig Speicherplatz	Diese Benachrichtigung informiert Sie darüber, dass vRealize Log Insight zu wenig zugewiesenen Speicherplatz hat. Diese Benachrichtigung weist darauf hin, dass bei vRealize Log Insight wahrscheinlich ein mit dem Speicher in Verbindung stehendes Problem vorliegt.
Archivplatz bald voll	Diese Benachrichtigung informiert Sie darüber, dass der für die Archivierung von vRealize Log Insight-Daten verwendete Speicherplatz auf dem NFS-Server bald ausgeschöpft ist.
Änderung des insgesamt bereitgestellten Festplattenspeichers	Diese Benachrichtigung informiert Sie darüber, dass sich die Gesamtgröße der Partition für die Speicherung von vRealize Log Insight-Daten verringert hat. Dies deutet in der Regel auf ein ernstes Problem im zugrunde liegenden Speichersystem hin. Wenn vRealize Log Insight diesen Umstand erkennt, wird diese Benachrichtigung in folgender Weise gesendet: <ul style="list-style-type: none"> ■ Sofort ■ Einmal pro Tag
Ausstehende Archivierungen	Diese Benachrichtigung informiert Sie darüber, dass vRealize Log Insight Daten nicht erwartungsgemäß archivieren kann. Die Benachrichtigung weist in der Regel auf Probleme mit dem von Ihnen für die Datenarchivierung konfigurierten NFS-Speicher hin.
Lizenz bald abgelaufen	Diese Benachrichtigung informiert Sie darüber, dass die vRealize Log Insight-Lizenz bald abläuft.
Lizenz ist abgelaufen	Diese Benachrichtigung informiert Sie darüber, dass die vRealize Log Insight-Lizenz abgelaufen ist.
Keine Verbindung mit dem AD-Server möglich	Diese Benachrichtigung informiert Sie darüber, dass vRealize Log Insight keine Verbindung zum konfigurierten Active Directory-Server herstellen kann.

Benachrichtigungsname	Beschreibung
<p>High Availability-IP-Adresse [IP-Adresse] kann nicht übernommen werden, da sie bereits von einer anderen Maschine verwendet wird</p>	<p>Diese Benachrichtigung informiert Sie darüber, dass der vRealize Log Insight-Cluster die für den integrierten Lastausgleichsdienst konfigurierte IP-Adresse nicht übernehmen konnte. Die häufigste Ursache für diese Warnung ist, dass ein anderer Host in demselben Netzwerk die IP-Adresse belegt, sodass sie nicht vom Cluster übernommen werden kann.</p> <p>Sie können diesen Konflikt lösen, indem Sie entweder die IP-Adresse auf dem Host, der sie belegt, freigeben oder den integrierten Log Insight-Lastausgleichsdienst mit einer im Netz verfügbaren statischen IP-Adresse versehen. Wenn Sie die IP-Adresse des integrierten Log Insight-Lastausgleichsdienstes ändern, müssen Sie alle Clients so konfigurieren, dass sie Protokolldaten an die neue IP-Adresse oder an einen FQDN bzw. eine URL senden, der bzw. die in diese IP-Adresse aufgelöst wird. Zudem müssen Sie von der vSphere-Integrationsseite aus die Konfiguration aller in vRealize Log Insight integrierten vCenter Server aufheben und diese neu konfigurieren.</p>

Benachrichtigungsname	Beschreibung
<p>High Availability-IP-Adresse [IP-Adresse] ist aufgrund zu vieler Knotenausfälle nicht verfügbar</p>	<p>Diese Benachrichtigung informiert Sie darüber, dass die IP-Adresse für den konfigurierten integrierten Lastausgleichsdienst nicht verfügbar ist. Das bedeutet, dass Clients, die Protokolldaten über die IP-Adresse des integrierten Lastausgleichsdienstes oder einen FQDN bzw. eine URL an den vRealize Log Insight-Cluster senden, der bzw. die in diese IP-Adresse aufgelöst wird, die IP-Adresse als nicht verfügbar sehen. Die häufigste Ursache für diese Warnung ist, dass die Mehrheit der Knoten im vRealize Log Insight-Cluster nicht ordnungsgemäß arbeiten, nicht verfügbar oder vom Master-Knoten aus nicht erreichbar sind. Eine weitere geläufige Ursache ist, dass die NTP-Zeitsynchronisation nicht aktiviert wurde oder es bei den konfigurierten NTP-Servern erhebliche Zeitabweichungen gibt. Sie können feststellen, ob das Problem noch besteht, indem Sie die IP-Adresse anpingen (sofern erlaubt) und prüfen, ob die Adresse nicht erreichbar ist. Sie können dieses Problem beheben, indem Sie sichergehen, dass ein Großteil der Clusterknoten ordnungsgemäß arbeitet und erreichbar ist, und die NTP-Zeitsynchronisation mit genauen NTP-Servern aktivieren.</p>
<p>Zu viele Migrationen der High Availability-IP-Adresse [Ihre IP-Adresse] zwischen vRealize Log Insight-Knoten</p>	<p>Diese Benachrichtigung informiert Sie darüber, dass die für den integrierten Lastausgleichsdienst konfigurierte IP-Adresse innerhalb der letzten 10 Minuten zu oft migriert wurde. Im Normalbetrieb bewegt sich die IP-Adresse nur selten zwischen vRealize Log Insight-Clusterknoten. Die IP-Adresse kann jedoch verschoben werden, wenn der aktuelle Besitzerknoten neu gestartet oder in die Wartung versetzt wird. Der andere Grund wäre eine unzureichende Zeitsynchronisierung zwischen Log Insight-Clusterknoten, was für das ordnungsgemäße Funktionieren des Clusters unerlässlich ist. In diesem Fall können Sie das Problem beheben, indem Sie die NTP-Uhrzeitsynchronisierung mit genauen NTP-Servern ermöglichen.</p>

Benachrichtigungsname	Beschreibung
SSL-Zertifikatsfehler	<p>Diese Benachrichtigung informiert Sie darüber, dass eine Syslog-Quelle eine Verbindung zu vRealize Log Insight über SSL initiiert, die Verbindung aber plötzlich abgebrochen hat. Dies weist möglicherweise darauf hin, dass die Syslog-Quelle die Gültigkeit des SSL-Zertifikats nicht bestätigen kann. Damit vRealize Log Insight Syslog-Nachrichten über SSL annehmen kann, ist ein Zertifikat erforderlich, welches vom Client validiert wird, und die Uhren des Systems müssen synchronisiert werden. Es liegt möglicherweise ein Problem mit dem SSL-Zertifikat oder mit dem Netzwerkzeitdienst vor.</p> <p>Sie können validieren, dass das SSL-Zertifikat für Ihre Syslog-Quelle vertrauenswürdig ist, die Quelle so neu konfigurieren, dass SSL nicht verwendet wird, oder das SSL-Zertifikat neu installieren. Siehe Konfigurieren der SSL-Parameter für vRealize Log Insight-Agenten und Installieren eines benutzerdefinierten SSL-Zertifikats.</p>
Fehler bei vCenter-Erfassung	<p>Diese Benachrichtigung informiert Sie darüber, dass vRealize Log Insight keine vCenter-Ereignisse, -Aufgaben und -Alarme erfassen kann. In der Datei <code>/storage/var/loginsight/plugins/vsphere/li-vsphere.log</code> finden Sie den genauen Fehler, der den Erfassungsfehler verursacht hat, und Sie können prüfen, ob die Erfassung korrekt läuft.</p>

Benachrichtigungsname	Beschreibung
Ereignisse für Ereignisweiterleitung gelöscht	<p>Diese Systembenachrichtigung wird gesendet, wenn eine Weiterleitung Ereignisse aus Verbindungs- oder Überlastungsgründen löscht.</p> <p>Beispiel:</p> <pre>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>
Verspätete Warnabfragen	Diese Benachrichtigung informiert Sie darüber, dass vRealize Log Insight zur konfigurierten Zeit keine Benutzerwarnung ausführen konnte. Die Verspätung ist möglicherweise auf eine oder mehrere ineffiziente Benutzerwarnungen oder eine unangemessene Systemgröße für das Erfassungs- und Abfragevolumen zurückzuführen.
Automatisch deaktivierte Warnung	Wenn eine Warnung mindestens zehnmal ausgeführt wurde und die durchschnittliche Zeit für die Ausführung länger als eine Stunde beträgt, wird die Warnung als ineffizient eingestuft und deaktiviert, um die Beeinträchtigung anderer Benutzerwarnungen zu verhindern.
Ineffiziente Warnabfrage	Wenn eine Warnung zum Abschließen länger als eine Stunde benötigt, wird die Warnung als ineffizient eingestuft.

Systembenachrichtigungen für Cluster

vRealize Log Insight sendet Benachrichtigungen über Änderungen der Clustertopologie, etwa durch Hinzufügen von neuen Clustermitgliedern oder vorübergehende Kommunikationsprobleme mit Knoten.

Gesendet von	Benachrichtigungsname	Beschreibung
Master-Knoten	Genehmigung für neuen Worker-Knoten erforderlich	Diese Benachrichtigung informiert Sie über eine Mitgliedschaftsanforderung von einem Worker-Knoten. Die Anforderung muss von einem Admin-Benutzer genehmigt oder abgelehnt werden.
Master-Knoten	Neuer Worker-Knoten genehmigt	Diese Benachrichtigung informiert Sie darüber, dass ein Admin-Benutzer eine Mitgliedschaftsanforderung von einem Worker-Knoten für den Beitritt zu einem vRealize Log Insight-Cluster genehmigt hat.
Master-Knoten	Neuer Worker-Knoten abgelehnt	Diese Benachrichtigung informiert Sie darüber, dass ein Admin-Benutzer eine Mitgliedschaftsanforderung von einem Worker-Knoten für den Beitritt zu einem vRealize Log Insight-Cluster abgelehnt hat. Sollte die Anforderung versehentlich abgelehnt worden sein, kann ein Admin-Benutzer diese über den Worker erneut ausgeben und sie anschließend im Master-Knoten genehmigen.
Master-Knoten	Maximale Anzahl unterstützter Knoten durch Worker-Knoten überschritten	Diese Benachrichtigung informiert Sie darüber, dass die maximal unterstützte Anzahl an Worker-Knoten im Log Insight-Cluster aufgrund eines neuen Worker-Knotens überschritten wurde.
Master-Knoten	Zulässige Höchstzahl an Knoten überschritten, neuer Worker-Knoten abgelehnt	Diese Benachrichtigung informiert Sie darüber, dass ein Admin-Benutzer versucht hat, dem Cluster mehr Knoten hinzuzufügen als maximal zulässig und dass der Knoten abgelehnt wurde.
Master-Knoten	Worker-Knoten getrennt	Diese Benachrichtigung informiert Sie darüber, dass ein zuvor verbundener Worker-Knoten vom vRealize Log Insight-Cluster getrennt wurde.
Master-Knoten	Worker-Knoten erneut verbunden	Diese Benachrichtigung informiert Sie darüber, dass ein Worker-Knoten wieder mit dem vRealize Log Insight-Cluster verbunden wurde.
Master-Knoten	Worker-Knoten von Admin widerrufen	Diese Benachrichtigung informiert Sie darüber, dass ein Admin-Benutzer die Mitgliedschaft eines Worker-Knotens widerrufen hat und der Knoten nicht mehr Teil des vRealize Log Insight-Clusters ist.

Gesendet von	Benachrichtigungsname	Beschreibung
Master-Knoten	Unbekannter Worker-Knoten abgelehnt	Diese Benachrichtigung informiert Sie darüber, dass der vRealize Log Insight-Master-Knoten die Anforderung eines Worker-Knotens abgelehnt hat, weil der Worker-Knoten dem Master-Knoten nicht bekannt war. Handelt es sich bei dem Worker-Knoten um einen gültigen Knoten, der dem Cluster hinzugefügt werden soll, melden Sie sich beim Worker-Knoten an, entfernen Sie dessen Token-Datei und Benutzerkonfiguration unter <code>/storage/core/loginsight/config/</code> und führen Sie im Worker-Knoten <code>restart loginsight service</code> aus.
Master-Knoten	Worker-Knoten ist in den Wartungsmodus übergegangen	Diese Benachrichtigung informiert Sie darüber, dass ein Worker-Knoten in den Wartungsmodus übergegangen ist und ein Admin-Benutzer den Wartungsmodus für den Worker-Knoten deaktivieren muss, bevor Änderungen an der Konfiguration des Worker-Knotens vorgenommen werden können und dieser Abfragen verarbeiten kann.
Master-Knoten	Worker-Knoten wieder betriebsbereit	Diese Benachrichtigung informiert Sie darüber, dass ein Worker-Knoten den Wartungsmodus verlassen hat und wieder betriebsbereit ist.

Gesendet von	Benachrichtigungsname	Beschreibung
Worker-Knoten	Master ausgefallen oder vom Worker-Knoten getrennt	<p>Diese Benachrichtigung informiert Sie darüber, dass ein Worker-Knoten, der die Benachrichtigung sendet, keinen Kontakt zum vRealize Log Insight-Master-Knoten herstellen kann. Dies könnte möglicherweise bedeuten, dass der Master-Knoten ausgefallen ist und gegebenenfalls neu gestartet werden muss. Bei einem Ausfall des Master-Knotens kann der Cluster nicht konfiguriert werden und es können keine Abfragen übermittelt werden, bis dieser wieder online ist. Worker-Knoten nehmen weiterhin Nachrichten auf.</p> <p>Hinweis Sie könnten möglicherweise viele solcher Benachrichtigungen erhalten, weil mehrere Worker-Knoten den Ausfall des Master-Knotens unabhängig voneinander registrieren und entsprechende Benachrichtigungen ausgeben könnten.</p>
Worker-Knoten	Master-Knoten mit Worker-Knoten verbunden	<p>Diese Benachrichtigung informiert Sie darüber, dass ein Worker-Knoten, der die Benachrichtigung sendet, wieder mit dem vRealize Log Insight-Master-Knoten verbunden ist.</p>

Konfigurieren von vRealize Log Insight - Systembenachrichtigungen

Administratoren können vRealize Log Insight-Systembenachrichtigungen so konfigurieren, dass Systembenachrichtigungen an Drittanbieteranwendungen und E-Mails an bestimmte Benutzer gesendet werden, wenn eine Benachrichtigung ausgelöst wird.

vRealize Log Insight erstellt diese Benachrichtigungen, wenn ein wichtiges Systemereignis auftritt, zum Beispiel wenn der Speicherplatz fast erschöpft ist und vRealize Log Insight alte Protokolldateien löschen oder archivieren muss.

Konfigurieren von vRealize Log Insight zum Senden von Benachrichtigungen über den Systemzustand


Administratoren können vRealize Log Insight so konfigurieren, dass Benachrichtigungen zum eigenen Systemzustand versendet werden.

Wenn eine E-Mail nicht übermittelt werden kann, werden Sie in der Web-Benutzeroberfläche über den Fehler benachrichtigt.

Voraussetzungen

- 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.
- Stellen Sie sicher, dass der SMTP-Server für vRealize Log Insight konfiguriert ist. Weitere Informationen finden Sie unter [Konfigurieren des SMTP-Servers für vRealize Log Insight](#).

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Configuration, click **General**.
- 3 Stellen Sie unter dem Warnungs-Header die Systembenachrichtigungen ein.
 - a Geben Sie im Textfeld **E-Mail-Versand von Systembenachrichtigungen an** die E-Mail-Adressen ein, an die eine Benachrichtigung gesendet werden soll.
Trennen Sie mehrere E-Mail-Adressen durch Kommata.
 - b Aktivieren Sie das Kontrollkästchen **Schwellenwert für Vorhaltezeitbenachrichtigung** und legen Sie den Schwellenwert fest, der die Benachrichtigungen auslöst.

Eine Benachrichtigung wird gesendet, wenn der Umfang an Daten, den das System aufnehmen kann, für den angegebenen Zeitraum nicht ausreicht. Dieser Wert wird basierend auf der aktuellen Aufnahmerate berechnet.
- 4 Click **Save**.
- 5 Click **Restart Log Insight** to apply your changes.

vRealize Log Insight -Systembenachrichtigungen für Drittanbieterprodukte konfigurieren


Administratoren können vRealize Log Insight so konfigurieren, dass Zustandsbenachrichtigungen an Drittanbieteranwendungen versendet werden.

vRealize Log Insight erstellt diese Benachrichtigungen, wenn ein wichtiges Systemereignis auftritt – etwa wenn der Speicherplatz fast erschöpft ist und vRealize Log Insight alte Protokolldateien löschen muss.

Voraussetzungen

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.

Vorgehensweise

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

- 3 Stellen Sie unter dem Warnungs-Header die Systembenachrichtigungen ein.
 - a Geben Sie im Textfeld **HTTP Post-Systembenachrichtigungen senden an** die URLs zur Benachrichtigung ein.
 - b (Optional) Bestätigen Sie, dass das Kontrollkästchen **Senden einer Benachrichtigung beim Absinken der Kapazität unter** sowie der damit verbundene Schwellenwert für Ihre Umgebung richtig konfiguriert sind.
- 4 Click **Save**.

Weiter

Erstellen Sie beim Arbeiten mit der Webhook-Ausgabe für Ihre Benachrichtigung einen Shim, um das vRealize Log Insight-Webhookformat dem von der Drittanbieteranwendung verwendeten Format zuzuordnen.

Informationen zur Verwendung von Webhooks zum Senden von Systembenachrichtigungen an Drittanbieterprodukte

Sie können vRealize Log Insight-Systembenachrichtigungen mithilfe von Webhooks an Drittanbieterprodukte senden.

vRealize Log Insight verwendet Webhooks, um Warnungen über HTTP POST an andere Anwendungen zu senden. vRealize Log Insight sendet einen Webhook in einem eigenen proprietären Format; von Drittanbieterlösungen wird aber erwartet, dass eingehende Webhooks ihr proprietäres Format aufweisen. Um mit vRealize Log Insight-Webhooks gesendete Informationen zu verwenden, muss die Drittanbieteranwendung entweder das vRealize Log Insight-Format nativ unterstützen oder Sie müssen mit einem Shim eine Zuordnung zwischen den vRealize Log Insight-Formaten und dem vom Drittanbieter verwendeten Format erstellen. Der Shim übersetzt das vRealize Log Insight-Format in ein anderes Format bzw. ordnet die Formate einander zu.

Systembenachrichtigungen, mit Meldungsabfragen erstellte Warnungen und mit aggregierten Abfragen erstellte Warnungen haben alle ihre eigenen Webhookformate.

Sie müssen vRealize Log Insight-Administrator sein, um Systembenachrichtigungen erstellen zu können.

Die HTTP-Standardauthentifizierung wird unterstützt. Betten Sie Anmeldedaten in der URL in der Form `{{https://Benutzername:Kennwort@Hostname/Pfad}}` ein.

Webhookformat für eine Systembenachrichtigung

Das Format eines vRealize Log Insight-Webhooks ist abhängig vom Abfragetyp, aus dem es erstellt wird. Systembenachrichtigungen, Warnungsmeldungsabfragen durch Benutzer und Warnungen, die aus aggregierten Benutzerabfragen generiert werden, haben alle ihre eigenen Webhookformate.

Sie müssen vRealize Log Insight -Administrator sein, um vRealize Log Insight für das Senden von Systembenachrichtigungen zu konfigurieren.

Wenn Sie eine Systembenachrichtigung an ein Drittanbieterprogramm senden, müssen Sie einen Shim schreiben, damit die vRealize Log Insight-Informationen von den Programmformaten des Drittanbieterprogramms verstanden werden.

Webhookformat für Systembenachrichtigungen

Das folgende Beispiel zeigt das vRealize Log Insight-Webhookformat für Systembenachrichtigungen.

```
{
  "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": []
    }
  ]
}
```

Hinzufügen eines Ziels für die vRealize Log Insight - Ereignisweiterleitung

Sie können einen vRealize Log Insight-Server auf die Weiterleitung eingehender Ereignisse an ein Syslog- oder Ingestion-API-Ziel konfigurieren.

Verwenden Sie die Ereignisweiterleitung für das Senden gefilterter oder getaggtter Ereignisse an ein oder mehrere Remoteziele wie z. B. vRealize Log Insight und/oder Syslog. Die Ereignisweiterleitung kann zur Unterstützung von vorhandenen Protokollierungstools wie z. B. SIEM und zur Konsolidierung der Protokollierung über verschiedene Netzwerke wie z. B. DMZ oder WAN verwendet werden.


Hinweis Ereignisweiterleitungen können unabhängig oder geclustert durchgeführt werden. Sie stellen aber immer eine vom Remoteziel unabhängige Instanz dar. Für die Ereignisweiterleitung konfigurierte Instanzen speichern Ereignisse auch lokal und können zur Abfrage von Daten verwendet werden.

Voraussetzungen

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.

Stellen Sie sicher, dass das Ziel die Anzahl der weitergeleiteten Ereignisse verarbeiten kann. Wenn das Zielcluster viel kleiner als die Weiterleitungsinstanz ist, werden manche Ereignisse eventuell gelöscht.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Klicken Sie unter „Verwaltung“ auf **Ereignisweiterleitung**.

3 Klicken Sie auf **Neues Ziel** und geben Sie die im Folgenden aufgeführten Informationen ein.

Option	Beschreibung
Name	Der eindeutige Name des neuen Ziels
Host	<p>Die IP-Adresse oder der vollständig qualifizierte Domänenname</p> <p>Vorsicht Eine Weiterleitungsschleife ist eine Konfiguration, bei der ein vRealize Log Insight-Cluster Ereignisse an sich selbst oder einen anderen Cluster weiterleitet, von dem die Ereignisse dann an den ursprünglichen Cluster zurückgeleitet werden. Durch eine solche Schleife kann unter Umständen eine unbegrenzte Anzahl an Kopien jedes weitergeleiteten Ereignisses erstellt werden. Die vRealize Log Insight-Web-Benutzeroberfläche erlaubt keine Konfiguration eines Ereignisses, das an sich selbst weitergeleitet wird. vRealize Log Insight kann jedoch keine indirekten Weiterleitungsschleifen verhindern, beispielsweise wenn vRealize Log Insight-Cluster A Ereignisse an Cluster B weiterleitet und Cluster B dieselben Ereignisse zurück an Cluster A sendet. Achten Sie bei der Erstellung von Weiterleitungszielen darauf, keine indirekten Weiterleitungsschleifen zu erstellen.</p>
Protokoll	<p>Ingestion-API oder Syslog. Die Standardeinstellung ist Ingestion-API (CFAPI). Wenn Ereignisse mithilfe der Ingestion-API weitergeleitet werden, wird die ursprüngliche Quelle des Ereignisses im Quellfeld beibehalten. Wenn Ereignisse mithilfe von Syslog weitergeleitet werden, geht die ursprüngliche Quelle des Ereignisses verloren und der Empfänger nimmt die Quelle der Nachricht als IP-Adresse oder Hostname der vRealize Log Insight-Ereignisweiterleitung auf.</p> <p>Hinweis Je nach auf der Ereignisweiterleitung ausgewähltem Protokoll kann das Quellfeld unterschiedliche Werte aufweisen:</p> <ul style="list-style-type: none"> a Für die Ingestion-API stellt die IP-Adresse des anfänglichen Senders (Erzeuger des Ereignisses) die Quelle dar. b Für syslog ist die Quelle die IP-Adresse der vRealize Log Insight-Instanz der Ereignisweiterleitung. Zudem enthält der Text der Syslog-Nachricht <code>_li_source_path</code>, der auf die IP-Adresse des anfänglichen Senders verweist.
SSL verwenden	<p>Sie können optional die Verbindung für die Ingestion-API mit SSL sichern. Das vertrauenswürdige Stammzertifikat des Remote-Servers wird validiert. Hierbei funktioniert die Ereignisweiterleitung mit SSL nicht mit selbstsignierten Zertifikaten, die standardmäßig auf Zielservern installiert sind. Ist ein Zertifikat nicht vertrauenswürdig, importieren Sie das vertrauenswürdige Stammzertifikat des Remote-Servers in den Keystore der Weiterleitungsinstanz. Weitere Informationen hierzu finden Sie unter Konfigurieren der vRealize Log Insight-Ereignisweiterleitung mit SSL.</p>
Tags	<p>Optional können Sie Tag-Paare mit vordefinierten Werten hinzufügen. Mit Tags lassen sich Ereignisse einfacher abfragen. Sie können mehrere durch Kommas getrennte Tags hinzufügen.</p>

Option	Beschreibung
Ergänzende Tags weiterleiten	Sie können auswählen, ob ergänzende Tags für Syslog weitergeleitet werden sollen. Ergänzende Tags sind Tags, die vom Cluster selbst hinzugefügt werden, wie beispielsweise „Vc_username“ oder „Vc_vmname“. Diese können zusammen mit den direkt aus Quellen stammenden Tags weitergeleitet werden. Ergänzende Tags werden immer weitergeleitet, wenn die Ingestion-API verwendet wird.
Transport	Wählen Sie ein Transportprotokoll für Syslog aus. Sie können das UDP- oder das TCP-Protokoll auswählen.

- 4 (Optional) Um die Ereignisse anzugeben, die weitergeleitet werden sollen, klicken Sie auf **+ Filter hinzufügen**.

Wählen Sie die Felder und die Einschränkungen aus, die die gewünschten Ereignisse definieren. Nur statische Felder können als Filter verwendet werden. Wenn Sie keinen Filter auswählen, werden alle Ereignisse weitergeleitet. Sie können durch Klicken auf **In „Interaktive Analyse“ ausführen** die Ergebnisse des erstellten Filters anzeigen.

Option	Beschreibung
entspricht	Mit dieser Option werden alle Zeichenfolgen ermittelt, die der angegebenen Zeichenfolge inklusive Platzhaltern entsprechen. Beispielsweise werden mit der Festlegung von Test* Zeichenfolgen wie Test123 und Testlauf gefunden, aber nicht die Zeichenfolge MeinTestlauf . Test ermittelt Test , aber nicht Test123 .
entspricht nicht	Mit dieser Option werden alle Zeichenfolgen ermittelt, die nicht der angegebenen Zeichenfolge inklusive Platzhaltern entsprechen. Beispielsweise wird mit Test* die Zeichenfolge Test123 ausgeschlossen, die Zeichenfolge MeinTest123 aber gefunden.
beginnt mit	Mit dieser Option werden alle Zeichenfolgen ermittelt, die mit den angegebenen Zeichen beginnen. Beispielsweise werden mit der Festlegung von Test die Zeichenfolgen Test123 und Test gefunden, aber nicht die Zeichenfolge MeinTest123 .
beginnt nicht mit	Mit dieser Option werden alle Zeichenfolgen ermittelt, die nicht mit den angegebenen Zeichen beginnen. Beispielsweise wird mit Test die Zeichenfolge Test123 ausgeschlossen, die Zeichenfolge „MeinTest123“ aber gefunden.

- 5 (Optional) Klicken Sie auf **Erweiterte Einstellungen anzeigen**, um die im Folgenden aufgeführten Weiterleitungsinformationen zu ändern.

Option	Beschreibung
Port	Der Port, an den die Ereignisse im Remoteziel gesendet werden. Die Standardeinstellung wird anhand des angegebenen Protokolls festgelegt. Ändern Sie sie nur, wenn das Remoteziel einen anderen Port überwacht.
Festplatten-Cache	Die Menge an lokalem Festplattenspeicher, die zur Zwischenspeicherung der weiterzuleitenden Ereignisse reserviert wird. Die Zwischenspeicherung wird verwendet, wenn das Remoteziel nicht verfügbar ist oder die empfangenen Ereignisse nicht verarbeiten kann. Wenn der lokale Puffer voll und das Remoteziel weiterhin nicht verfügbar ist, werden die letzten lokalen Ereignisse gelöscht und nicht an das Remoteziel weitergeleitet, auch wenn später das Remoteziel wieder online ist. Die Standardeinstellung ist 200 MB.
Anzahl Worker	Die verwendete Anzahl gleichzeitiger ausgehender Verbindungen. Geben Sie eine höhere Anzahl von Workern an, um einer höheren Netzwerklatenz zum weitergeleiteten Ziel Rechnung zu tragen und um mehr Ereignisse pro Sekunde weiterzuleiten. Der Standardwert lautet 8.

- 6 Klicken Sie zum Prüfen Ihrer Konfiguration auf **Test**.

- 7 Klicken Sie auf **Speichern**.

Weiter

- [Konfigurieren der vRealize Log Insight-Ereignisweiterleitung mit SSL](#).
- Ereignisweiterleitungsziele können bearbeitet oder geklont werden. Wenn Sie das Ziel so bearbeiten, dass der Name einer Ereignisweiterleitung geändert wird, werden sämtliche Statistiken zurückgesetzt.

Konfigurieren der vRealize Log Insight -Ereignisweiterleitung mit SSL

Sie können einen vRealize Log Insight-Server für die Weiterleitung eingehender Ereignisse an einen anderen Log Insight-Server anhand des Ingestion-API-Ziels mit SSL konfigurieren.

Voraussetzungen

Die Ereignisweiterleitung mit SSL funktioniert nicht mit dem selbstsignierten Zertifikat, das standardmäßig auf den Zielserversn installiert ist. Ein benutzerdefiniertes SSL-Zertifikat muss anhand der unter [Generieren einer Zertifizierungsanforderung](#) aufgeführten Schritte erstellt und anschließend hochgeladen werden. Siehe [Installieren eines benutzerdefinierten SSL-Zertifikats](#).

Vorgehensweise

- 1 Kopieren Sie das vertrauenswürdige Stammzertifikat in ein temporäres Verzeichnis auf der Weiterleitungsinstanz. Beispiel: /home.

- 2 SSH an die Weiterleitungsinstanz, und führen Sie die folgenden Befehle aus.

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

Das Standard-Keystore-Kennwort ist **changeit**.

Hinweis Java-Versionen können mit der Zeit variieren.

- 3 Starten Sie die vRealize Log Insight-Instanz neu.

Wenn Sie eine vRealize Log Insight-Clusterumgebung verwenden, muss dieser Vorgang auf allen Knoten mit demselben Zertifikat durchgeführt werden.

Weiter

Aktivieren Sie die SSL-Verbindung. Weitere Informationen hierzu finden Sie unter [SSL-Verbindungen erzwingen](#).

Synchronisieren der Uhrzeit der virtuellen vRealize Log Insight -Appliance

Die Uhrzeit der virtuellen vRealize Log Insight-Appliance muss mit einem NTP-Server oder dem ESX-/ESXi-Host, auf dem Sie die virtuelle Appliance bereitgestellt haben, synchronisiert werden.


Die Uhrzeit ist für die Kernfunktionalität von vRealize Log Insight von entscheidender Bedeutung.

vRealize Log Insight synchronisiert standardmäßig die Uhrzeit mit einer vordefinierten Liste öffentlicher NTP-Server. Sollten öffentliche NTP-Server aufgrund einer Firewall nicht zugänglich sein, können Sie den internen NTP-Server Ihres Unternehmens nutzen. Wenn keine NTP-Server verfügbar sind, können Sie die Uhrzeit mit dem ESX-/ESXi-Host, auf dem Sie die virtuelle vRealize Log Insight-Appliance bereitgestellt haben, synchronisieren.

Voraussetzungen

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.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Klicken Sie unter „Konfiguration“ auf **Uhrzeit**.

- 3 Wählen Sie im Dropdown-Menü **Uhrzeit synchronisieren mit** die Zeitquelle aus.

Option	Beschreibung
NTP-Server	Synchronisiert die Uhrzeit der virtuellen vRealize Log Insight-Appliance mit der Uhrzeit eines der aufgeführten NTP-Server.
ESX/ESXi-Host	Synchronisiert die Uhrzeit der virtuellen vRealize Log Insight-Appliance mit dem ESX-/ESXi-Host, auf dem Sie die virtuelle Appliance bereitgestellt haben.

- 4 (Optional) Wenn Sie NTP-Server-Synchronisation ausgewählt haben, listen Sie die NTP-Server-Adressen auf und klicken Sie auf **Testen**.

Hinweis Das Testen der Verbindung zu NTP-Servern kann bis zu 20 Sekunden pro Server in Anspruch nehmen.

- 5 Click **Save**.

Konfigurieren des SMTP-Servers für vRealize Log Insight


Sie können einen SMTP so konfigurieren, dass das Versenden von E-Mail-Warnungen durch vRealize Log Insight zugelassen wird.

Systemwarnungen werden erzeugt, wenn vRealize Log Insight ein wichtiges Systemereignis erkennt, zum Beispiel wenn die Speicherkapazität der virtuellen Appliance die von Ihnen festgelegten Schwellenwerte erreicht.

Voraussetzungen

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.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Klicken Sie unter "Konfiguration" auf **SMTP**.
- 3 Geben Sie die SMTP-Server-Adresse und die Portnummer ein.
- 4 Wenn der SMTP-Server eine verschlüsselte Verbindung verwendet, wählen Sie das Verschlüsselungsprotokoll aus.
- 5 Geben Sie im Textfeld **Absender** eine E-Mail-Adresse ein, die beim Versenden von Systemwarnungen verwendet werden soll.

Die **Absender**-Adresse erscheint als die Adresse des Absenders in den Systembenachrichtigungs-E-Mails. Sie muss keine echte Adresse sein und kann durch ihren Namen auf eine spezifische Instanz von vRealize Log Insight hinweisen. Beispiel: **loginsight@beispiel.com**.

- 6 Geben Sie einen Benutzernamen und ein Kennwort zur Authentifizierung beim SMTP-Server beim Versenden von Systemwarnungen ein.

- 7 Geben Sie eine Ziel-E-Mail-Adresse ein und klicken Sie auf **Test-E-Mail senden**, um die Verbindung zu überprüfen.
- 8 Click **Save**.

Installieren eines benutzerdefinierten SSL-Zertifikats

Standardmäßig installiert vRealize Log Insight ein selbstsigniertes SSL-Zertifikat auf der virtuellen Appliance.

Das selbstsignierte Zertifikat generiert Sicherheitswarnungen, wenn Sie eine Verbindung mit der vRealize Log Insight-Web-Benutzeroberfläche herstellen. Wenn Sie kein selbstsigniertes Sicherheitszertifikat verwenden möchten, können Sie ein benutzerdefiniertes SSL-Zertifikat installieren. Die einzige Funktion, die ein benutzerdefiniertes SSL-Zertifikat benötigt, ist „Ereignisweiterleitung über SSL“. Wenn Sie über ein Cluster-Setup mit ILB-Aktivierung verfügen, finden Sie unter [Aktivieren des integrierten Lastausgleichsdiensts](#) die spezifischen Anforderungen für ein benutzerdefiniertes SSL-Zertifikat.

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

Voraussetzungen

- 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.
- Verketteten Sie den gesamten Textkörper jedes einzelnen Zertifikats in einer einzelnen Textdatei in der folgenden Reihenfolge.
 - a Privater Schlüssel: `ihr_domänennamen.key`
 - b Hauptzertifikat: `ihr_domänennamen.crt`
 - c Zwischenzertifikat: `DigiCertCA.crt`

d Stammzertifikat: *TrustedRoot.crt*

- Die öffnenden und schließenden Tags jedes Zertifikats müssen in folgendem Format vorliegen.

```
-----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.

Vorgehensweise

1 Generieren eines selbstsignierten Zertifikats

Sie können mit dem OpenSSL-Tool ein selbstsigniertes Zertifikat für Windows oder Linux generieren.

2 Generieren einer Zertifizierungsanforderung

Generieren Sie eine Zertifizierungsanforderung über das OpenSSL-Tool für Windows.

3 Anfordern einer Signatur von einer Zertifizierungsstelle

Senden Sie Ihre Zertifizierungsanforderung an eine Zertifizierungsstelle Ihrer Wahl und fordern Sie eine Signatur an.

4 Verketteten von Zertifikatsdateien

Verknüpfen Sie Ihre Schlüssel- und Zertifikatsdateien in einer PEM-Datei.

5 Hochladen des signierten Zertifikats

Sie können ein signiertes SSL-Zertifikat hochladen.

6 Konfigurieren der SSL-Verbindung zwischen dem vRealize Log Insight-Server und den Log Insight Agents

Mit der SSL-Funktion können Sie über den sicheren Fluss der Ingestion-API reine SSL-Verbindungen zwischen Log Insight Agents und dem vRealize Log Insight-Server bereitstellen. Sie können zudem eine Vielzahl von SSL-Parametern von den Log Insight Agents konfigurieren.

Generieren eines selbstsignierten Zertifikats

Sie können mit dem OpenSSL-Tool ein selbstsigniertes Zertifikat für Windows oder Linux generieren.

Voraussetzungen

- Laden Sie das entsprechende Installationsprogramm für OpenSSL auf <https://www.openssl.org/community/binaries.html> herunter. Verwenden Sie das heruntergeladene OpenSSL-Installationsprogramm, um es auf Windows zu installieren.
- Bearbeiten Sie die Datei `openssl.cnf`, um weitere erforderliche Parameter hinzuzufügen. Stellen Sie sicher, dass der Parameter `req_extensions` im Abschnitt `[req]` definiert ist.

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

- Fügen Sie einen adäquaten Eintrag „Alternativer Antragstellername“ für den Hostnamen oder die IP-Adresse Ihres Servers hinzu, wie beispielsweise `server-01.loginsight.domain`. Für den Hostnamen können Sie kein Muster festlegen.

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

Vorgehensweise

- 1 Erstellen Sie einen Ordner, in dem Ihre Zertifikatsdateien gespeichert werden sollen, zum Beispiel `C:\Certs\LogInsight`.
- 2 Öffnen Sie eine Eingabeaufforderung und führen Sie den folgenden Befehl aus.

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

OpenSSL fordert zur Eingabe von Zertifikatseigenschaften, einschließlich Land, Organisation usw., auf.

- 3 Geben Sie die IP-Adresse oder den Hostnamen Ihres vRealize Log Insight-Servers oder die vRealize Log Insight-Clusteradresse ein, wenn Lastausgleich aktiviert ist.

Diese Eigenschaft ist die einzige, für die ein Wert angegeben werden muss.

Es werden zwei Dateien erstellt: `server.key` und `server.crt`.

- `server.key` ist ein neuer PEM-verschlüsselter privater Schlüssel.
- `server.crt` ist ein neues PEM-verschlüsseltes, von `server.key` signiertes Zertifikat.

Weiter

- Verketteten Sie die Zertifikatsdateien. Weitere Informationen hierzu finden Sie unter [Verketten von Zertifikatsdateien](#).
- Laden Sie das signierte Zertifikat hoch. Weitere Informationen hierzu finden Sie unter [Hochladen des signierten Zertifikats](#).

Generieren einer Zertifizierungsanforderung

Generieren Sie eine Zertifizierungsanforderung über das OpenSSL-Tool für Windows.

Voraussetzungen

- Laden Sie das entsprechende Installationsprogramm für OpenSSL auf <http://www.openssl.org/related/binaries.html> herunter. Verwenden Sie das heruntergeladene OpenSSL-Installationsprogramm, um es auf Windows zu installieren.
- Bearbeiten Sie die Datei `openssl.cnf`, um weitere erforderliche Parameter hinzuzufügen. Stellen Sie sicher, dass der Parameter `req_extensions` im Abschnitt `[req]` definiert ist.

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

- Fügen Sie einen adäquaten Eintrag „Alternativer Antragstellername“ für den Hostnamen oder die IP-Adresse Ihres Servers hinzu, wie beispielsweise `server-01.loginsight.domain`. Für den Hostnamen können Sie kein Muster festlegen.

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

Vorgehensweise

- 1 Erstellen Sie einen Ordner, in dem Ihre Zertifikatsdateien gespeichert werden sollen, zum Beispiel `C:\Certs\LogInsight`.
- 2 Öffnen Sie eine Eingabeaufforderung und führen Sie den folgenden Befehl aus, um Ihren privaten Schlüssel zu generieren:

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

- 3 Erstellen Sie eine Zertifizierungsanforderung, indem Sie den folgenden Befehl ausführen:

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

Hinweis Dieser Befehl wird interaktiv ausgeführt und es werden Ihnen eine Reihe von Fragen gestellt. Ihre Antworten werden durch Ihre Zertifizierungsstelle überprüft. Ihre Antworten müssen den Angaben der mit der Eintragung Ihres Unternehmens verbundenen Rechtsdokumente entsprechen.

- 4 Folgen Sie den Anweisungen auf dem Bildschirm und geben Sie die Informationen ein, die in Ihren Zertifikatsantrag aufgenommen werden.

Wichtig Geben Sie im Feld „Common Name“ (Allgemeiner Name) den Hostnamen oder die IP-Adresse des Servers an, zum Beispiel **mail.your.domain**. Wenn Sie alle Subdomains einschließen möchten, geben Sie ***your.domain** ein.

Ihre Zertifizierungsanforderungsdatei `server.csr` wird generiert und gespeichert.

Anfordern einer Signatur von einer Zertifizierungsstelle

Senden Sie Ihre Zertifizierungsanforderung an eine Zertifizierungsstelle Ihrer Wahl und fordern Sie eine Signatur an.

Vorgehensweise

- ◆ Senden Sie Ihre `server.csr`-Datei an eine Zertifizierungsstelle.

Hinweis Beantragen Sie bei der Zertifizierungsstelle, Ihre Datei im PEM-Format codieren zu lassen.

Die Zertifizierungsstelle bearbeitet Ihre Anforderung und sendet Ihnen eine im PEM-Format codierte `server.crt`-Datei zurück.

Verketteten von Zertifikatsdateien

Verknüpfen Sie Ihre Schlüssel- und Zertifikatsdateien in einer PEM-Datei.

Vorgehensweise

- 1 Erstellen Sie eine neue `server.pem`-Datei und öffnen Sie sie in einem Texteditor.
- 2 Kopieren Sie den Inhalt Ihrer `server.key`-Datei und fügen Sie ihn mit dem folgenden Format in die `server.pem`-Datei ein.

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

- 3 Kopieren Sie den Inhalt Ihrer `server.crt`-Datei und fügen Sie ihn mit dem folgenden Format in die `server.pem`-Datei ein.

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

- 4 Wenn die Zertifizierungsstellen Ihnen ein Zwischenzertifikat oder ein verkettetes Zertifikat ausgestellt haben, fügen Sie die Zwischenzertifikate oder verketteten Zertifikate im folgenden Format am Ende der öffentlichen Zertifikatsdatei an.


```
-----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 Speichern Sie Ihre `server.pem`-Datei.

Hochladen des signierten Zertifikats

Sie können ein signiertes SSL-Zertifikat hochladen.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Klicken Sie unter „Konfiguration“ auf **SSL-Zertifikat**.
- 3 Suchen Sie Ihr benutzerdefiniertes SSL-Zertifikat und klicken Sie auf **Öffnen**.
- 4 Click **Save**.
- 5 Starten Sie vRealize Log Insight neu.

Weiter

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](#).

Konfigurieren der SSL-Verbindung zwischen dem vRealize Log Insight -Server und den Log Insight Agents

Mit der SSL-Funktion können Sie über den sicheren Fluss der Ingestion-API reine SSL-Verbindungen zwischen Log Insight Agents und dem vRealize Log Insight-Server bereitstellen. Sie können zudem eine Vielzahl von SSL-Parametern von den Log Insight Agents konfigurieren.

vRealize Log Insight-Agenten kommunizieren über TLSv.1.2. SSLv.3/TLSv.1.0 ist zur Erfüllung von Sicherheitsrichtlinien deaktiviert.

SSL-Hauptfunktionen

Das Verstehen der wesentlichen SSL-Funktionen kann Ihnen bei der ordnungsgemäßen Konfiguration von Log Insight Agents helfen.

Der vRealize Log Insight-Agent speichert Zertifikate und nutzt diese dann zur Verifizierung der Serveridentität bei allen Verbindungen mit einem bestimmten Server mit Ausnahme der allerersten Verbindung. Wenn sich die Serveridentität nicht bestätigen lässt, weist der vRealize Log Insight-Agent die Verbindung mit dem Server ab und vermerkt eine entsprechende Fehlermeldung im Protokoll. Die vom Agent empfangenen Zertifikate werden im Ordner cert gespeichert.

- Navigieren Sie unter Windows zu `C:\ProgramData\VMware\Log Insight Agent\cert`.
- Navigieren Sie unter Linux zu `/var/lib/loginsight-agent/cert`.

Wenn der vRealize Log Insight-Agent eine sichere Verbindung mit dem vRealize Log Insight-Server hergestellt hat, prüft der Agent das vom vRealize Log Insight-Server erhaltene Zertifikat auf seine Gültigkeit. Der vRealize Log Insight-Agent nutzt Stammzertifikate, denen das System vertraut.

- Der Log Insight Linux Agent lädt die vertrauenswürdigen Zertifikate von `/etc/pki/tls/certs/ca-bundle.crt` oder `/etc/ssl/certs/ca-certificates.crt`.
- Der Log Insight Windows Agent nutzt System-Stammzertifikate.

Wenn der vRealize Log Insight-Agent über ein lokal gespeichertes, selbstsigniertes Zertifikat verfügt und ein anderes gültiges, selbstsigniertes Zertifikat mit demselben öffentlichen Schlüssel empfängt, akzeptiert der Agent das neue Zertifikat. Dies kann bei der Neuerstellung eines selbstsignierten Zertifikats unter Verwendung desselben privaten Schlüssels, jedoch mit anderen Details, wie einem neuen Ablaufdatum, geschehen. Ansonsten wird die Verbindung abgewiesen.

Wenn der vRealize Log Insight-Agent über ein lokal gespeichertes, selbstsigniertes Zertifikat verfügt und ein gültiges, von einer Zertifizierungsbehörde (CA) signiertes Zertifikat empfängt, ersetzt der vRealize Log Insight-Agent stillschweigend das neue akzeptierte Zertifikat.

Wenn der vRealize Log Insight-Agent das selbstsignierte Zertifikat empfängt, nachdem er ein von einer Zertifizierungsbehörde (CA) signiertes Zertifikat erhalten hat, wird es vom Log Insight Agent zurückgewiesen. Der vRealize Log Insight-Agent akzeptiert das selbstsignierte, vom vRealize Log Insight-Server empfangene Zertifikat nur bei der ersten Verbindung mit dem Server.

Wenn der vRealize Log Insight-Agent über ein lokal gespeichertes, von einer Zertifizierungsbehörde (CA) signiertes Zertifikat verfügt und ein gültiges, von einer anderen vertrauenswürdigen Zertifizierungsbehörde (CA) signiertes Zertifikat erhält, wird dieses vom Agent zurückgewiesen. Sie können die Konfigurationsoptionen des vRealize Log Insight-Agents so modifizieren, dass dieser das neue Zertifikat annimmt. Weitere Informationen hierzu finden Sie unter [Konfigurieren der SSL-Parameter für vRealize Log Insight-Agenten](#).

vRealize Log Insight-Agenten kommunizieren über TLSv.1.2. SSLv.3/TLSv.1.0 ist zur Erfüllung von Sicherheitsrichtlinien deaktiviert.

SSL-Verbindungen erzwingen


Sie können die vRealize Log Insight-Web-Benutzeroberfläche verwenden, um die vRealize Log Insight Agents und die Ingestion-API so zu konfigurieren, dass nur SSL-Verbindungen mit dem Server zugelassen werden.

Die vRealize Log Insight-API kann normalerweise über HTTP über den Port 9000 und über HTTPS über den Port 9543 erreicht werden. Beide Ports können vom vRealize Log Insight-Agent oder benutzerdefinierten API-Clients verwendet werden. Für alle authentifizierten Anforderungen ist SSL erforderlich. Nicht authentifizierte Anforderungen, einschließlich Erfassungsdatenverkehr über den vRealize Log Insight-Agent, können mit oder ohne SSL erfolgen. Sie können alle API-Anforderungen zwingen, SSL-Verbindungen zu verwenden. Dies führt zu keiner Einschränkung des Datenverkehrs über Syslog-Port 514 und hat keinen Einfluss auf die vRealize Log Insight-Benutzeroberfläche, für die Anforderungen an HTTP-Port 80 weiterhin an HTTPS-Port 443 weitergeleitet werden.

Voraussetzungen

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.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Klicken Sie unter „Konfiguration“ auf **SSL**.
- 3 Wählen Sie unter „API-Server-SSL“ die Einstellung **SSL-Verbindung erforderlich**.
- 4 Click **Save**.

Die vRealize Log Insight-API gestattet nur SSL-Verbindungen zu dem Server. Nicht-SSL-Verbindungen werden abgewiesen.

Konfigurieren der SSL-Parameter für vRealize Log Insight -Agenten

Sie können die Konfigurationsdatei des vRealize Log Insight-Agenten bearbeiten, um die SSL-Konfiguration zu ändern, den vertrauenswürdigen Rootzertifikaten einen Pfad hinzuzufügen und festzulegen, ob Zertifikate vom Agenten akzeptiert werden.

Dieses Verfahren gilt für die vRealize Log Insight-Agenten für Windows und Linux.

Voraussetzungen

Für den Linux-Agenten von vRealize Log Insight:

- Melden Sie sich als **Root**-Benutzer an oder verwenden Sie `sudo`, um Konsolenbefehle auszuführen.
- Melden Sie sich bei dem Linux-System an, auf dem Sie den vRealize Log Insight-Linux-Agenten installiert haben. Öffnen Sie eine Konsole und führen Sie `pgrep liagent` aus, um sicherzustellen, dass der vRealize Log Insight-Linux-Agent installiert ist und ausgeführt wird.

Für den Windows-Agenten von vRealize Log Insight:

- 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.

Vorgehensweise

- 1 Navigieren Sie zum Ordner mit der Datei `liagent.ini`.

Betriebssystem	Pfad
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 Fügen Sie dem `[server]`Abschnitt der Datei `liagent.ini` die folgenden Schlüssel hinzu.

Schlüssel	Beschreibung
<code>ssl_ca_path</code>	<p>Überschreibt den Standardspeicherpfad für von der Stammzertifizierungsstelle signierte Zertifikate, die für die Überprüfung von Verbindungs-Peer-Zertifikaten verwendet werden.</p> <p>Linux: Wenn kein Wert angegeben ist, versucht der Agent, vertrauenswürdige Zertifikate von der Datei <code>/etc/pki/tls/certs/ca-bundle.crt</code> oder von der Datei <code>/etc/ssl/certs/ca-certificates.crt</code> zu laden.</p> <p>Windows: Wenn kein Wert angegeben ist, lädt der vRealize Log Insight-Windows-Agent Zertifikate aus dem Windows-Stammzertifikatspeicher.</p> <p>Wenn für <code>ssl_ca_path</code> ein Pfad angegeben ist, überschreibt dieser die Standardeinstellungen sowohl für Linux- wie für Windows-Agenten. Sie können als Wert eine Datei angeben, in der mehrere Zertifikate im PEM-Format verknüpft sind, oder ein Verzeichnis, das Zertifikate im PEM-Format und Namen in der Form <code>hash.0</code> (siehe <code>-hash</code>-Option des <code>x509</code>-Dienstprogramms) enthält.</p>
<code>ssl_accept_any</code>	<p>Legt fest, ob Zertifikate vom vRealize Log Insight-Agenten akzeptiert werden. Die möglichen Werte sind <code>yes</code>, <code>1</code>, <code>no</code> oder <code>0</code>. Wenn der Wert auf „Ja“ oder <code>1</code> festgelegt ist, akzeptiert der Agent jegliche Zertifikate vom Server und richtet eine sichere Verbindung zum Versenden von Daten ein. Der Standardwert lautet „Nein“.</p>

Schlüssel	Beschreibung
ssl_accept_any_trusted	Die möglichen Werte sind Ja, 1, Nein oder 0. Wenn der vRealize Log Insight-Agent über ein lokal gespeichertes, von einer vertrauenswürdigen Zertifizierungsstelle signiertes Zertifikat verfügt und ein anderes gültiges Zertifikat empfängt, das von einer anderen vertrauenswürdigen Zertifizierungsstelle signiert ist, prüft er die Konfigurationsoption. Ist der Wert auf „Ja“ oder 1 festgelegt, akzeptiert der Agent das neue gültige Zertifikat. Ist der Wert auf „Nein“ oder 0 festgelegt, lehnt er das Zertifikat ab und beendet die Verbindung. Der Standardwert lautet „Nein“.
ssl_cn	Der Common Name des selbstsignierten Zertifikats. Der Standardwert lautet VMware vCenter Log Insight. Sie können einen benutzerdefinierten Common Name festlegen, auf den das Feld Common Name des Zertifikats geprüft werden muss. Der vRealize Log Insight-Agent überprüft das Feld Common Name des empfangenen Zertifikats auf den Hostnamen, der für den Schlüssel hostname im Bereich [server] angegeben wurde. Gibt es keine Übereinstimmung, prüft der Agent das Feld Common Name auf den Schlüssel ssl_cn in der Datei liagent.ini. Stimmen die Werte überein, akzeptiert der vRealize Log Insight-Agent das Zertifikat.

Hinweis Diese Schlüssel werden ignoriert, wenn SSL deaktiviert ist.

- 4 Save and close the liagent.ini file.

Beispiel: Konfiguration

Es folgt ein Beispiel für eine SSL-Konfiguration.

```
proto=capi
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
```

Ändern des Standard-Zeitlimits für vRealize Log Insight - Websitzungen


Zur Gewährleistung der Sicherheit Ihrer Umgebung laufen vRealize Log Insight-Websitzungen nach 30 Minuten ab. Sie können das Zeitlimit erhöhen oder verringern.

Das Zeitlimit kann über die Web-Benutzeroberfläche geändert werden.

Voraussetzungen

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.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Configuration, click **General**.
- 3 Geben Sie im Bereich „Browsersitzung“ ein Zeitlimit in Minuten an.
Der Wert –1 deaktiviert Sitzungszeitlimits.
- 4 Click **Save**.

Archive

Aktivieren oder Deaktivieren der Datenarchivierung in vRealize Log Insight

Durch Datenarchivierung werden alte Protokolle aufbewahrt, die aus Speicherplatzgründen möglicherweise von der virtuellen vRealize Log Insight-Appliance entfernt werden könnten. vRealize Log Insight kann archivierte Daten als NFS-Mounts speichern.

vRealize Log Insight erfasst und speichert Protokolle in einer Reihe von 1-GB-Buckets auf der Festplatte. Ein Bucket besteht aus komprimierten Protokolldateien und einem Index. Es enthält alles, was zur Durchführung von Abfragen in einem bestimmten Zeitraum notwendig ist. Sobald die Größe eines Bucket 1 GB erreicht, unterbricht vRealize Log Insight die Speicherung, schließt alle Dateien im Bucket und verschließt das Bucket.

Wenn Sie die Datenarchivierung nutzen, kopiert vRealize Log Insight beim Verschließen des Bucket die unverarbeiteten komprimierten Protokolldateien aus dem Bucket in einen NFS-Mount. Buckets, die bei deaktivierter Datenarchivierung verschlossen wurden, werden nicht nachträglich archiviert.


Der innerhalb eines Archivexportvorgangs erstellte Pfad liegt im Format **jahr/monat/tag/stunde/behälter-uuid/daten.blob** vor, wobei der Zeitstempel der ursprünglichen Behältererstellung in UTC verwendet wird.

Hinweis vRealize Log Insight verwaltet den für Archivierungszwecke verwendeten NFS-Mount nicht. Wenn Systembenachrichtigungen aktiviert sind, sendet vRealize Log Insight eine E-Mail, wenn der NFS-Mount bald über keinen freien Speicherplatz mehr verfügt oder nicht zur Verfügung steht. Wenn der NFS-Mount nicht über ausreichend freien Speicherplatz verfügt oder länger als die Aufbewahrungszeit der virtuellen Appliance nicht verfügbar ist, stellt vRealize Log Insight die Erfassung neuer Daten ein. Die Erfassung neuer Daten beginnt wieder, wenn für den NFS-Mount genügend freier Speicherplatz vorhanden, der NFS-Mount verfügbar oder die Archivierung deaktiviert ist.

Voraussetzungen

- Stellen Sie sicher, dass Sie Zugriff auf eine den folgenden Anforderungen entsprechende NFS-Partition haben.
 - Die NFS-Partition muss Lese- und Schreibvorgänge für Gastkonten ermöglichen.
 - Für den Mount darf keine Authentifizierung erforderlich sein.
 - Der NFS-Server muss NFS v3 unterstützen.
 - Wenn Sie einen Windows NFS-Server verwenden, aktivieren Sie die Option „UNIX-Zugriff durch nicht zugeordneten Benutzer zulassen (über 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.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Klicken Sie unter „Konfiguration“ auf **Archivieren**.
- 3 Wählen Sie **Datenarchivierung aktivieren** aus und geben Sie den Pfad einer NFS-Partition, auf der Protokolle archiviert werden, im Format `nfs://Servername<:Portnummer>/Exportname` ein.
Die Portnummer lautet standardmäßig 2049.
- 4 Klicken Sie auf **Testverbindung**, um die Verbindung zu überprüfen.
- 5 Click **Save**.

Hinweis Durch Datenarchivierung werden Protokollereignisse aufbewahrt, die aus Speicherplatzgründen von der virtuellen vRealize Log Insight-Appliance entfernt wurden. Von der virtuellen vRealize Log Insight-Appliance entfernte Protokollereignisse, die archiviert wurden, können nicht mehr durchsucht werden. Wenn Sie archivierte Protokolle durchsuchen möchten, müssen Sie diese in eine vRealize Log Insight-Instanz importieren. Weitere Informationen zum Importieren von archivierten Protokolldateien finden Sie unter [Importieren eines vRealize Log Insight-Archivs in vRealize Log Insight](#).

Weiter

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 der vRealize Log Insight -Archivdateien

vRealize Log Insight archiviert Daten in einem bestimmten Format.

vRealize Log Insight speichert Archivdateien auf einem NFS-Server und organisiert diese in hierarchischen Verzeichnissen basierend auf der Archivierungszeit. Beispiel:

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

wobei es sich bei `/backup` um den NFS-Speicherort, bei `2014/08/07/16` um den Zeitpunkt der Archivierung, bei `bd234b2d-df98-44ae-991a-e0562f10a49` um die Bucket-ID und bei `data.blob` um die archivierten Daten für das Bucket handelt.

Die Archivdaten `data.blob` bestehen aus einer komprimierten Datei, die interne vRealize Log Insight-Codierung verwendet. Sie enthält den ursprünglichen Inhalt für alle im Bucket gespeicherten Nachrichten sowie die statischen Felder wie „timestamp“ und „host“. Name, Quelle und Anwendungsname.

Sie können archivierte Daten in vRealize Log Insight importieren, archivierte Daten in eine Rohtextdatei exportieren und Nachrichteninhalte aus Archivdaten extrahieren. Siehe [Exportieren eines Log Insight-Archivs in eine Rohtextdatei oder JSON](#) und [Importieren eines vRealize Log Insight-Archivs in vRealize Log Insight](#).

Importieren eines vRealize Log Insight -Archivs in vRealize Log Insight

Durch die Datenarchivierung werden alte Protokolle aufbewahrt, die aus Speicherplatzgründen möglicherweise von der virtuellen vRealize Log Insight-Appliance entfernt würden. Weitere Informationen hierzu finden Sie unter [Aktivieren oder Deaktivieren der Datenarchivierung in vRealize Log Insight](#). In vRealize Log Insight archivierte Protokolle können über die Befehlszeile importiert werden.

Hinweis Obwohl vRealize Log Insight historische und Echtzeitdaten gleichzeitig verarbeiten kann, empfiehlt es sich, für die Verarbeitung von importierten Protokolldateien eine separate Instanz von vRealize Log Insight einzusetzen.

Voraussetzungen

- Verify that you have the root user credentials to log in to the vRealize Log Insight virtual appliance.
- Stellen Sie sicher, dass Sie Zugriff auf den NFS-Server haben, auf dem die vRealize Log Insight-Protokolle archiviert werden.
- Vergewissern Sie sich, dass in der virtuellen Appliance für vRealize Log Insight genügend Speicherplatz für die importierten Protokolldateien vorhanden ist.

Der mindestens verfügbare Speicher in der Partition `/storage/core` der virtuellen Appliance muss mindestens 10-mal so groß sein wie das archivierte Protokoll, das importiert werden soll.

Vorgehensweise

- 1 Stellen Sie eine SSH-Verbindung zur vRealize Log Insight-vApp her und melden Sie sich als Root-Benutzer an.
- 2 Stellen Sie den freigegebenen Ordner auf dem NFS-Server bereit, auf dem die archivierten Daten vorliegen.

- 3 Zum Importieren eines Verzeichnisses von archivierten vRealize Log Insight-Protokollen führen Sie folgenden Befehl aus.

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

Hinweis Der Import der archivierten Daten kann je nach Größe des Importordners sehr lange dauern.

- 4 Schließen Sie die SSH-Verbindung.

Weiter

Sie können die importierten Protokollereignisse durchsuchen, filtern und analysieren.

Exportieren eines Log Insight-Archivs in eine Rohtextdatei oder JSON

Über die Befehlszeile können Sie ein vRealize Log Insight-Archiv in eine gewöhnliche reine Textdatei oder in das JSON-Format exportieren.

Hinweis Dieses Verfahren richtet sich an erfahrene Benutzer. Die Befehlssyntax und Ausgabeformate können sich in späteren Versionen von vRealize Log Insight ohne Rückwärtskompatibilität ändern.

Voraussetzungen

- Verify that you have the root user credentials to log in to the vRealize Log Insight virtual appliance.
- Vergewissern Sie sich, dass in der virtuellen Appliance für vRealize Log Insight genügend Speicherplatz für die exportierten Dateien vorhanden ist.

Vorgehensweise

- 1 Stellen Sie eine SSH-Verbindung zur vRealize Log Insight-vApp her und melden Sie sich als Root-Benutzer an.
- 2 Erstellen Sie ein Archivverzeichnis in der vApp für vRealize Log Insight.

```
mkdir /archive
```

- 3 Stellen Sie den freigegebenen Ordner auf dem NFS-Server bereit, auf dem die archivierten Daten vorliegen, indem Sie folgenden Befehl ausführen.

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

- 4 Prüfen Sie den verfügbaren Speicherplatz in der vApp für vRealize Log Insight.

```
df -h
```

5 Exportieren Sie ein vRealize Log Insight-Archiv in eine reine Textdatei.

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

Beispiel:

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

6 Exportieren Sie den Inhalt einer vRealize Log Insight-Archivmeldung in das JSON-Format.

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

Beispiel:

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

7 Schließen Sie die SSH-Verbindung.

Neustart des vRealize Log Insight -Dienstes


Sie können vRealize Log Insight über die Verwaltungsseite der Web-Benutzeroberfläche neu starten.

Vorsicht Bei einem Neustart von vRealize Log Insight werden alle aktiven Benutzersitzungen geschlossen. Benutzer der vRealize Log Insight-Instanz müssen sich erneut anmelden.

Voraussetzungen

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.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **Cluster**.
- 3 Wählen Sie einen Clusterknoten aus.
- 4 Klicken Sie auf **Master neu starten** und dann auf **Neu starten**.

Weiter

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](#).

Ausschalten der virtuellen vRealize Log Insight - Appliance

Um beim Ausschalten eines vRealize Log Insight-Master- oder Worker-Knotens einen Datenverlust zu vermeiden, müssen Sie den Knoten in einer strengen Abfolge von Schritten ausschalten.

Sie müssen die virtuelle vRealize Log Insight-Appliance ausschalten, bevor Sie Änderungen an der virtuellen Hardware der Appliance vornehmen.

Sie können die virtuelle vRealize Log Insight-Appliance über die Menüoption **Betrieb > Gast herunterfahren** in vSphere Client, mithilfe der Konsole der virtuellen Appliance oder durch Herstellung einer SSH-Verbindung zur virtuellen vRealize Log Insight-Appliance und Ausführung eines Befehls ausschalten.

Voraussetzungen

- 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.

Vorgehensweise

- 1 Stellen Sie eine SSH-Verbindung zur vRealize Log Insight-vApp her und melden Sie sich als Root-Benutzer an.
- 2 Führen Sie zum Ausschalten der virtuellen vRealize Log Insight-Appliance `shutdown -h now` aus.

Weiter

Sie können sicher Änderungen an der virtuellen Hardware der virtuellen vRealize Log Insight-Appliance vornehmen.

Herunterladen eines Support-Pakets für vRealize Log Insight


Falls vRealize Log Insight aufgrund eines Problems nicht wie erwartet funktioniert, können Sie eine Kopie der Protokoll- und Konfigurationsdateien in Form eines Support-Pakets an die Support-Dienste von VMware senden.

Der Download eines clusterübergreifenden Support-Pakets ist nur bei einer Aufforderung durch die Support-Dienste von VMware erforderlich. Sie können das Paket entweder statisch erstellen, wodurch Festplattenspeicher auf dem Knoten verwendet wird, oder durch Streamen, wodurch kein Festplattenspeicher auf dem Knoten verwendet und das Paket standardmäßig auf der zur Erstellung verwendeten Maschine gespeichert wird.

Voraussetzungen

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.

Vorgehensweise

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

2 Klicken Sie unter „Verwaltung“ auf **Cluster**.

3 Klicken Sie unter dem Support-Header auf **Support-Paket herunterladen**.

Das vRealize Log Insight-System erfasst die Diagnoseinformationen und sendet die Daten in einer komprimierten TAR-Datei an Ihren Browser.

4 Wählen Sie die Methode zur Erstellung des Pakets.

- Wählen Sie **Statisches Support-Paket**, um ein lokales Paket zu erstellen. Durch die Erstellung des Pakets wird Festplattenspeicher auf dem Knoten verwendet.
- Wählen Sie **Support-Paket streamen**, um sofort mit dem Streamen des Support-Pakets zu beginnen. Durch diese Methode wird kein Speicherplatz auf dem Knoten belegt.

5 Klicken Sie auf **Fortfahren**.

6 Klicken Sie im Dialogfeld „Datei-Download“ auf **Speichern**.

7 Wählen Sie das Verzeichnis aus, in dem Sie das Tarball-Archiv speichern möchten, und klicken Sie auf **Speichern**.

Weiter

Sie können den Inhalt der Protokolldateien auf Fehlermeldungen überprüfen. Wenn Sie Probleme behoben haben, löschen Sie das veraltete Support-Paket, um Festplattenspeicher freizugeben.

Teilnahme am VMware-Programm zur Verbesserung der Benutzerfreundlichkeit oder Verlassen des Programms


Nach der Bereitstellung von vRealize Log Insight können Sie am VMware-Programm zur Verbesserung der Benutzerfreundlichkeit teilnehmen oder das Programm verlassen.

Sie können bei der Installation von vRealize Log Insight entscheiden, ob Sie am Programm zur Verbesserung der Benutzerfreundlichkeit teilnehmen möchten oder nicht. Führen Sie die folgenden Schritte aus, um nach der Installation an dem Programm teilzunehmen oder es zu verlassen.

Voraussetzungen

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.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Configuration, click **General**.
- 3 Aktivieren bzw. deaktivieren Sie im Bereich „Programm zur Verbesserung der Benutzerfreundlichkeit“ das Kontrollkästchen **Am VMware-Programm zur Verbesserung der Benutzerfreundlichkeit teilnehmen**.

Wenn diese Option aktiviert ist, wird das Programm aktiviert und es werden Daten an <https://vmware.com> gesendet.

- 4 Click **Save**.

Konfigurieren von vRealize Log Insight-Clustern

5

Sie können Knoten eines vRealize Log Insight-Clusters hinzufügen, entfernen und aktualisieren.

Hinweis Das WAN-Clustering wird von vRealize Log Insight nicht unterstützt. Aktuelle Versionen von vRealize Log Insight unterstützen das WAN-Clustering nicht (dies wird auch als Geo-Clustering, Hochverfügbarkeits-Clustering oder Remote-Clustering bezeichnet). Alle Knoten im Cluster müssen in demselben Layer 2-LAN bereitgestellt werden. Darüber hinaus müssen die unter [Ports und externe Schnittstellen](#) beschriebenen Ports zwischen den Knoten geöffnet sein, um eine ordnungsgemäße Kommunikation zu gewährleisten.

Dieses Kapitel behandelt die folgenden Themen:

- [Hinzufügen eines Worker-Knotens zu einem vRealize Log Insight-Cluster](#)
- [Entfernen eines Worker-Knotens aus einem vRealize Log Insight-Cluster](#)
- [Arbeiten mit einem integrierten Lastausgleichsdienst](#)
- [Abfragen der Ergebnisse von Clusterprüfungen in der Produktion](#)

Hinzufügen eines Worker-Knotens zu einem vRealize Log Insight -Cluster

Stellen Sie eine neue Instanz der virtuellen Log Insight-Appliance bereit und fügen Sie sie einem vorhandenen Log Insight-Master-Knoten hinzu.

Vorgehensweise

1 [Bereitstellen der virtuellen vRealize Log Insight-Appliance](#)

Laden Sie die virtuelle vRealize Log Insight-Appliance herunter. VMware verteilt die virtuelle vRealize Log Insight-Appliance als .ova-Datei. Stellen Sie die virtuelle vRealize Log Insight-Appliance mithilfe von vSphere Client bereit.

2 [Hinzufügen zu einer vorhandenen Bereitstellung](#)

Nach Bereitstellung und Einrichtung eines eigenständigen vRealize Log Insight-Knotens können Sie eine neue vRealize Log Insight-Instanz bereitstellen und diese dem vorhandenen Knoten hinzufügen, um einen vRealize Log Insight -Cluster zu bilden.

Bereitstellen der virtuellen vRealize Log Insight -Appliance

Laden Sie die virtuelle vRealize Log Insight-Appliance herunter. VMware verteilt die virtuelle vRealize Log Insight-Appliance als .ova-Datei. Stellen Sie die virtuelle vRealize Log Insight-Appliance mithilfe von vSphere Client bereit.

Voraussetzungen

- Vergewissern Sie sich, dass Sie über eine Kopie der .ova-Datei der virtuellen vRealize Log Insight-Appliance verfügen.
- Vergewissern Sie sich, dass Sie über die Berechtigungen verfügen, die OVF-Vorlagen in der Bestandsliste bereitzustellen.
- Überprüfen Sie, ob Ihre Umgebung über genügend Ressourcen verfügt, um die Mindestanforderungen der virtuellen vRealize Log Insight-Appliance zu erfüllen. Weitere Informationen hierzu finden Sie unter [Mindestanforderungen](#).
- Bestätigen Sie, dass Sie die Dimensionierungsempfehlungen für die virtuelle Appliance gelesen und verstanden haben. Siehe [Dimensionierung der virtuellen Log Insight-Appliance](#).

Vorgehensweise

- 1 Wählen Sie in vSphere Client die Option **Datei > OVF-Vorlage bereitstellen**.
- 2 Folgen Sie den Eingabeaufforderungen im **Assistenten zum Bereitstellen von OVF-Vorlagen**.
- 3 Wählen Sie auf der Seite „Konfiguration auswählen“ die Größe der virtuellen vRealize Log Insight-Appliance auf Basis der Größe der Umgebung, für die Sie Protokolle erfassen möchten.

Klein ist die Mindestanforderung für Produktionsumgebungen.

vRealize Log Insight bietet voreingestellte VM-Größen, aus denen Sie auswählen können, um die Erfassungsanforderungen Ihrer Umgebung zu erfüllen. Bei diesen voreingestellten Größen handelt es sich um zertifizierte Größenkombinationen von Berechnungs- und Festplattenressourcen.

Anschließend können jedoch weitere Ressourcen hinzugefügt werden. Eine kleine Konfiguration verbraucht bei andauernder Unterstützung die wenigsten Ressourcen. Eine extra kleine Konfiguration ist nur für Demos geeignet.

Option	Protokollaufnahmerate	Virtuelle CPUs	Arbeitsspeicher	IOPS	Syslog-Verbindungen (aktive TCP-Verbindungen)	Ereignisse pro Sekunde
Extra klein	6GB/Tag	2	4 GB	75	20	400
Klein	30GB/Tag	4	8 GB	500	100	2000

Option	Protokollaufnahmerate	Virtuelle CPUs	Arbeitsspeicher	IOPS	Syslog-Verbindungen (aktive TCP-Verbindungen)	Ereignisse pro Sekunde
Mittel	75GB/Tag	8	16 GB	1000	250	5000
Groß	225 GB/Tag	16	32 GB	1500	750	15,000

Hinweis Sie können einen Syslog-Aggregator verwenden, um die Anzahl der Syslog-Verbindungen zu erhöhen, die Ereignisse an vRealize Log Insight senden. Die Höchstanzahl der Ereignisse pro Sekunde ist jedoch fest und unabhängig vom Einsatz des Syslog-Aggregators. Eine vRealize Log Insight-Instanz lässt sich nicht als Syslog-Aggregator verwenden.

Hinweis Wenn Sie **Groß** wählen, müssen Sie die virtuelle Hardware auf der virtuellen Maschine von vRealize Log Insight nach der Bereitstellung aktualisieren.

4 Wählen Sie auf der Seite „Speicher auswählen“ ein Festplattenformat.

- **Thick-Provision Lazy-Zeroed** erstellt eine virtuelle Festplatte im Standard-Thick-Format. Der für die virtuelle Festplatte erforderliche Speicherplatz wird dann zugeteilt, wenn die virtuelle Festplatte erstellt wird. Die Daten, die auf dem physischen Gerät verbleiben, werden nicht während des Anlegens, sondern später während der ersten Schreibvorgänge der virtuellen Appliance gelöscht.
- **Thick-Provision Eager-Zeroed** erstellt einen Typ einer virtuellen Festplatte im Thick-Format, der Clusterfunktionen, wie z. B. Fault Tolerance, unterstützt. Der Speicher, den die virtuelle Festplatte benötigt, wird beim Erstellen zugewiesen. Im Gegensatz zum Flat-Format werden die auf dem physischen Gerät verbleibenden Daten durch Nullbyte ersetzt („zeroed out“), wenn die virtuelle Festplatte erstellt wird. Das Anlegen von Festplatten in diesem Format kann wesentlich länger dauern als das Anlegen anderer Festplattentypen.

Wichtig Stellen Sie, soweit möglich, die virtuelle vRealize Log Insight-Appliance mit Festplatten vom Typ Thick-Provisioned, Eager-Zeroed bereit, um Leistung und Betrieb der virtuellen Appliance zu optimieren.

- **Thin Provision** erstellt eine Festplatte im Thin-Format. Die Festplatte vergrößert sich mit anwachsendem Volumen der auf ihr gespeicherten Daten. Wenn Ihr Speichergerät keine Festplatten vom Typ Thick-Provisioning unterstützt oder Sie ungenutzten Speicherplatz auf der virtuellen vRealize Log Insight-Appliance einsparen möchten, stellen Sie die virtuelle Appliance mit Festplatten vom Typ Thin-Provisioning bereit.

Hinweis Das Verkleinern von Festplatten auf der virtuellen vRealize Log Insight-Appliance wird nicht unterstützt und kann zu Datenbeschädigung oder -verlust führen.

- 5 (Optional) Richten Sie auf der Seite „Netzwerk einrichten“ die Netzwerkparameter für die virtuelle vRealize Log Insight-Appliance ein.

Wenn Sie keine Netzwerkeinstellungen wie IP-Adresse, DNS-Server und Gateway-Informationen vornehmen, verwendet vRealize Log Insight DHCP, um diese Einstellungen vorzunehmen.

Vorsicht Geben Sie nicht mehr als zwei Domännennamenserver an. Wenn Sie mehr als zwei Domännennamenserver angeben, werden alle konfigurierten Domännennamenserver in der virtuellen vRealize Log Insight-Appliance ignoriert.

Verwenden Sie eine kommasetrennte Liste, um Domännennamen anzugeben.

- 6 (Optional) Richten Sie auf der Seite „Benutzerdefinierte Vorlage“ die Netzwerkeigenschaften ein, wenn Sie DHCP nicht verwenden.
- 7 (Optional) Wählen Sie auf der Seite „Benutzerdefinierte Vorlage“ **Sonstige Eigenschaften** aus und legen Sie das Root-Kennwort für die virtuelle vRealize Log Insight-Appliance fest.

Das Root-Kennwort ist erforderlich für SSH. Sie können das Kennwort auch über die VMware Remote Console festlegen.

- 8 Folgen Sie den Eingabeaufforderungen, um die Bereitstellung abzuschließen.

Informationen zur Bereitstellung virtueller Appliances finden Sie im *Benutzerhandbuch für die Bereitstellung von vApps und virtuellen Appliances*.

Nach dem Einschalten der virtuellen Appliance beginnt eine Initialisierung. Das Abschließen der Initialisierung kann unter Umständen mehrere Minuten dauern. Am Ende des Vorgangs erfolgt ein Neustart der virtuellen Appliance.

- 9 Gehen Sie zur Registerkarte **Konsole** und überprüfen Sie die IP-Adresse der virtuellen vRealize Log Insight-Appliance.

IP-Adresspräfix	Beschreibung
https://	Die DHCP-Konfiguration in der virtuellen Appliance ist korrekt.
http://	Die DHCP-Konfiguration in der virtuellen Appliance ist fehlgeschlagen. a Schalten Sie die virtuelle vRealize Log Insight-Appliance aus. b Klicken Sie mit der rechten Maustaste auf die virtuelle Appliance und wählen Sie Einstellungen bearbeiten . c Legen Sie eine statische IP-Adresse für die virtuelle Appliance fest.

Weiter

- Informationen zum Konfigurieren einer eigenständigen Bereitstellung von vRealize Log Insight finden Sie unter [Konfigurieren einer neuen Bereitstellung von 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.

Hinzufügen zu einer vorhandenen Bereitstellung

Nach Bereitstellung und Einrichtung eines eigenständigen vRealize Log Insight-Knotens können Sie eine neue vRealize Log Insight-Instanz bereitstellen und diese dem vorhandenen Knoten hinzufügen, um einen vRealize Log Insight -Cluster zu bilden.

vRealize Log Insight ermöglicht eine horizontale Skalierung durch den Einsatz mehrerer virtueller Appliance-Instanzen in Clustern. Cluster ermöglichen die lineare Skalierung des Aufnahmedurchsatzes, erhöhen die Abfrageleistung und erlauben eine Hochverfügbarkeitsaufnahme. Im Cluster-Modus bietet vRealize Log Insight Master- und Worker-Knoten. Master- und Worker-Knoten sind für eine Teilmenge von Daten verantwortlich. Master-Knoten können alle Teilmengen von Daten abfragen und die Ergebnisse aggregieren.

Wichtig Konfigurieren Sie in einem vRealize Log Insight-Cluster mindestens drei Knoten, um eine Aufnahme, eine Konfiguration und eine Hochverfügbarkeit des Benutzerspeicherplatzes zur Verfügung zu stellen.

Voraussetzungen

- Notieren Sie in vSphere Client die IP-Adresse der virtuellen vRealize Log Insight-Worker-Appliance.
- Sie müssen die IP-Adresse oder den Hostnamen der virtuellen vRealize Log Insight-Master-Appliance kennen.
- Stellen Sie sicher, dass Sie über ein Administratorkonto auf der virtuellen vRealize Log Insight-Master-Appliance verfügen.
- Stellen Sie sicher, dass die Versionen der vRealize Log Insight-Master- und Worker-Knoten synchron sind. Fügen Sie einem vRealize Log Insight-Master-Knoten einer neueren Version keinen vRealize Log Insight-Worker-Knoten einer älteren Version hinzu.
- Sie müssen die Uhrzeit der virtuellen vRealize Log Insight-Appliance mit einem NTP-Server synchronisieren. Siehe [Synchronisieren der Uhrzeit der virtuellen Log Insight-Appliance](#).
- Weitere Informationen über unterstützte Browserversionen finden Sie in den [Versionshinweise zu vRealize Log Insight](#).

Vorgehensweise

- 1 Verwenden Sie einen unterstützten Browser, um zur Web-Benutzeroberfläche des vRealize Log Insight-Workers zu navigieren.

Das URL-Format lautet `https://log_insight-host/`, wobei `log_insight-host` die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Worker-Appliance ist.

Der Erstkonfigurationsassistent wird geöffnet.

- 2 Klicken Sie auf **Hinzufügen zu einer vorhandenen Bereitstellung**.

- 3 Geben Sie die IP-Adresse oder den Hostnamen des vRealize Log Insight-Masters ein und klicken Sie auf **Los**.

Der Worker sendet eine Anforderung an den vRealize Log Insight-Master-Knoten, der vorhandenen Bereitstellung beizutreten.

- 4 Klicken Sie auf **Klicken Sie hier, um auf die Seite „Clusterverwaltung“ zuzugreifen**.

- 5 Melden Sie sich als Administrator an.

Die Cluster-Seite wird geladen.

- 6 Klicken Sie auf **Zulassen**.

Der Worker wird der vorhandenen Bereitstellung hinzugefügt und vRealize Log Insight wird als Cluster betrieben.

Weiter

- Stellen Sie, um einen weiteren Worker hinzuzufügen, eine neue vRealize Log Insight-Instanz bereit und fügen Sie diese über den Startassistenten dem Cluster hinzu.
- Wiederholen Sie das Verfahren, um mindestens zwei vRealize Log Insight-Worker-Knoten hinzuzufügen.

Entfernen eines Worker-Knotens aus einem vRealize Log Insight -Cluster

Sie können einen Worker-Knoten, der nicht mehr richtig arbeitet, aus einem vRealize Log Insight-Cluster entfernen und einem anderen Cluster hinzufügen oder eine eigenständige Bereitstellung starten.


Entfernen Sie keine Worker-Knoten, die ordnungsgemäß arbeiten, aus einem Cluster.

Das Entfernen eines Knotens führt zu Datenverlust. Wenn ein Knoten entfernt werden muss, stellen Sie sicher, dass er gesichert wurde. Warten Sie 30 Minuten nach dem Hinzufügen neuer Knoten, bevor Sie Knoten entfernen.

Voraussetzungen

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.


Vorgehensweise

- 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.

Hinweis A node in maintenance mode continues to receive logs.

- 4 Klicken Sie auf , um den Knoten zu entfernen.

vRealize Log Insight entfernt den Knoten aus dem Cluster und sendet eine E-Mail-Benachrichtigung.

Weiter

Navigieren Sie zur Web-Benutzeroberfläche des entfernten Knotens, um diesen zu konfigurieren. Sie können den Knoten einem anderen bestehenden vRealize Log Insight-Cluster hinzufügen oder eine neue eigenständige Bereitstellung starten.

Arbeiten mit einem integrierten Lastausgleichsdienst

Sie können den integrierten Lastausgleichsdienst von vRealize Log Insight (integrated load balancer, ILB) in einem vRealize Log Insight-Cluster aktivieren, um sicherzustellen, dass der eingehende Erfassungsdatenverkehr von vRealize Log Insight akzeptiert wird, selbst wenn einige vRealize Log Insight-Knoten nicht verfügbar sein sollten. Sie können auch mehrere virtuelle IP-Adressen konfigurieren.

Es wird dringend empfohlen, den integrierten Lastausgleichsdienst in einer vRealize Log Insight-Cluster-Umgebung für eine ordnungsgemäße Verteilung des Datenverkehrs auf die Knoten in einem Cluster zu aktivieren, um so den Verwaltungsaufwand zu minimieren.

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

Als Best Practice ist es empfehlenswert, den integrierten Lastausgleichsdienst in alle Bereitstellungen einzubeziehen, auch für Einzelknoteninstanzen. Senden Sie Abfragen und den Aufnahmeverkehr an den integrierten Lastausgleichsdienst, damit ein Cluster bei Bedarf problemlos in der Zukunft unterstützt werden kann.

Der integrierte Lastausgleichsdienst stellt sicher, dass der eingehende Aufnahmeverkehr von vRealize Log Insight akzeptiert wird, selbst wenn einige vRealize Log Insight-Knoten nicht verfügbar sein sollten. Außerdem verteilt der integrierte Lastausgleichsdienst den eingehenden Datenverkehr gleichmäßig auf alle verfügbaren vRealize Log Insight-Knoten. vRealize Log Insight-Clients, die sowohl die Web-Benutzeroberfläche als auch die Aufnahme (über Syslog oder die Ingestion-API) verwenden, sollten sich über die IP-Adresse des integrierten Lastausgleichsdiensts mit vRealize Log Insight verbinden.

Für den integrierten Lastausgleichsdienst müssen alle vRealize Log Insight-Knoten im selben Layer-2-Netzwerk liegen, beispielsweise hinter demselben Switch, oder auf sonstige Weise in der Lage sein, ARP-Anforderungen untereinander zu versenden oder zu empfangen. Die IP-Adresse des integrierten Lastausgleichsdiensts muss so eingerichtet sein, dass jeder vRealize Log Insight-Knoten über sie

Datenverkehr empfangen kann. Das bedeutet üblicherweise, dass sich die IP-Adresse des integrierten Lastausgleichsdiensts im selben Subnetz wie die physische Adresse der vRealize Log Insight-Knoten befindet. Nach der Konfiguration der IP-Adresse des integrierten Lastausgleichsdiensts versuchen Sie einen Ping von einem anderen Netzwerk aus, um sicherzugehen, dass sie erreicht werden kann.

Um zukünftige Änderungen und Upgrades möglichst einfach zu gestalten, können Clients auf einen FQDN verweisen, der die IP-Adresse des integrierten Lastausgleichsdiensts auflöst, anstatt direkt auf die IP-Adresse des integrierten Lastausgleichsdiensts zu verweisen.

Informationen zur Direct Server Return-Konfiguration

Der Lastausgleichsdienst von vRealize Log Insight verwendet eine Direct Server Return-Konfiguration (DSR-Konfiguration). Bei DSR passiert der gesamte eingehende Datenverkehr den vRealize Log Insight-Knoten, bei dem es sich um den aktuellen Lastausgleichsdienst-Knoten handelt, während der zurückgegebene Datenverkehr direkt von vRealize Log Insight-Servern zurück an den Client gesendet wird, ohne dafür den Lastausgleichsdienst-Knoten passieren zu müssen.

Mehrere virtuelle IP-Adressen

Sie können für den integrierten Lastausgleichsdienst mehrere virtuelle IP-Adressen (vIPs) konfigurieren. Sie können auch eine Liste mit statischen Tags für jede vIP so konfigurieren, dass jede von der vIP empfangene Protokollmeldung die konfigurierten Tags enthält.


Aktivieren des integrierten Lastausgleichsdiensts

Wenn Sie den integrierten Lastausgleichsdienst (integrated load balancer, ILB) von vRealize Log Insight auf einem vRealize Log Insight-Cluster aktivieren, können Sie eine oder mehrere virtuelle IP-Adressen konfigurieren. Optional können Sie Benutzern den Zugriff auf den Cluster über FQDN ermöglichen.

Voraussetzungen

- Überprüfen Sie, dass sich alle vRealize Log Insight-Knoten und die angegebene IP-Adresse des integrierten Lastausgleichsdiensts im selben Netzwerk befinden.
- Die Master- und Worker-Knoten von vRealize Log Insight müssen dieselben Zertifikate aufweisen. Andernfalls lehnen die vRealize Log Insight-Agenten, die für die Verbindung mit SSL konfiguriert sind, die Verbindung ab. Setzen Sie beim Hochladen eines von einer Zertifizierungsstelle signierten Zertifikats auf Master- und Worker-Knoten von vRealize Log Insight den allgemeinen Namen während der Zertifikatserstellungsanfrage auf die IP-Adresse des integrierten Lastausgleichsdiensts. Weitere Informationen hierzu finden Sie unter [Generieren einer Zertifizierungsanforderung](#).
- 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](#).

Vorgehensweise

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

- 3 Wählen Sie unter „Konfiguration“ die Option **Neue virtuelle IP-Adresse** aus und geben Sie die virtuelle IP-Adresse (vIP) für den integrierten Lastausgleich ein.
- 4 (Optional) Klicken Sie für das Konfigurieren mehrerer virtueller IP-Adressen auf **Neue virtuelle IP-Adresse** und geben Sie die IP-Adresse ein. Sie können den FQDN und Tags eingeben.
 - Jede vIP sollte sich auf jedem Knoten in demselben Subnetz befinden wie mindestens eine Netzwerkschnittstelle und die vIP muss verfügbar sein (d. h. nicht von einer anderen Maschine verwendet werden).
 - Mit Tags können Sie Ereignissen Felder mit vordefinierten Werten hinzufügen, um die Abfragen zu vereinfachen. Sie können mehrere durch Kommas getrennte Tags hinzufügen. Alle Ereignisse, die über eine vIP ins System gelangen, sind mit den Tags der vIP markiert.
 - Sie können eine Liste mit statischen Tags (Schlüssel=Wert) für die vIP eines ILB so konfigurieren, dass jede von der vIP empfangene Protokollmeldung die konfigurierten Tags enthält.
- 5 (Optional) Um Benutzern von vRealize Log Insight den Zugriff auf den Cluster über einen FQDN zu ermöglichen, verweisen Sie die Clients auf den FQDN anstatt direkt auf die konfigurierte IP-Adresse des integrierten Lastausgleichsdiensts.
- 6 Klicken Sie auf **Speichern**.

Der integrierte Lastausgleichsdienst wird von einem Knoten im vRealize Log Insight-Cluster verwaltet, der als Führungsknoten für den Dienst angegeben wird. Der aktuelle Führungsknoten wird durch den Text „(ILB)“ neben dem Knoten bezeichnet.

Abfragen der Ergebnisse von Clusterprüfungen in der Produktion

Der Dienst zur Clusterprüfung in der Produktion führt regelmäßig an jedem Knoten eine Reihe von Prüfungen durch. Sie können die neuesten Ergebnisse der Clusterprüfungen in der Produktion über die Befehlszeilenschnittstelle abfragen.

Der Dienst stellt beispielsweise fest, ob der Cluster wie erwartet läuft und konfiguriert ist, oder ob Probleme mit der Integration in andere Systeme bestehen. Zusätzliche Prüfungen sind unten aufgelistet.

- Ist NTP in einer Bereitstellung mit mehreren Hosts konfiguriert?
- Kann Active Directory erreicht werden (falls derzeit konfiguriert)?
- Ist die Active Directory-Authentifizierung möglich (falls derzeit konfiguriert)?
- Können die Active Directory-Hosts und die Kerberos-Hosts erreicht werden (wenn Active Directory derzeit konfiguriert ist)?
- Wird das System in einer nicht unterstützten Bereitstellung mit zwei Hosts ausgeführt?
- Ist genügend Speicherplatz in /tmp vorhanden, um ein Upgrade durchzuführen?
- Ist genügend Speicherplatz in /storage/core vorhanden, um ein Upgrade durchzuführen?
- Ist localhost richtig in /etc/hosts platziert?

Vorgehensweise

- 1 Stellen Sie an der Befehlszeile eine SSH-Verbindung zur virtuellen vRealize Log Insight-Appliance her und melden Sie sich als Root-Benutzer an.
- 2 Geben Sie an der Befehlszeile `/usr/lib/loginsight/application/sbin/query-check-results.sh` ein und drücken Sie die **Eingabetaste**.

Ports und externe Schnittstellen

vRealize Log Insight verwendet bestimmte erforderliche Dienste, Ports und externe Schnittstellen.

Kommunikationsports

vRealize Log Insight verwendet die Kommunikationsports und -protokolle, die in diesem Thema aufgeführt sind. Die erforderlichen Ports sind danach sortiert, ob sie für Quellen, für die Benutzeroberfläche, zwischen Clustern oder für externe Dienste erforderlich sind oder ob sie von einer Firewall auf sichere Weise blockiert werden können. Manche Ports werden nur verwendet, wenn Sie die entsprechende Integration aktivieren.

Hinweis vRealize Log Insight unterstützt das WAN-Clustering nicht (dies wird auch als Geo-Clustering, Hochverfügbarkeits-Clustering oder Remote-Clustering bezeichnet). Alle Knoten im Cluster müssen in demselben Layer 2-LAN bereitgestellt werden. Darüber hinaus müssen die in diesem Abschnitt beschriebenen Ports zwischen den Knoten geöffnet sein, um eine ordnungsgemäße Kommunikation zu gewährleisten.

Der Netzwerkdatenverkehr von vRealize Log Insight stammt aus verschiedenen Quellen.

Admin-Workstation	Die Maschine, die von einem Systemadministrator zur Fernverwaltung der virtuellen vRealize Log Insight-Appliance verwendet wird.
Benutzer-Workstation	Die Maschine, auf der ein Benutzer von vRealize Log Insight einen Browser für den Zugriff auf die Web-Oberfläche von vRealize Log Insight verwendet.
Protokolle sendendes System	Der Endpoint, der zu Analyse- und Suchzwecken Protokolle an vRealize Log Insight sendet. Solche Endpoints können z. B. ESXi-Hosts, virtuelle Maschinen oder jedes System mit einer IP-Adresse sein.
Log Insight Agents	Der Agent, der sich auf einer Windows- oder Linux-Maschine befindet und Ereignisse und Protokolle des Betriebssystems über APIs an vRealize Log Insight sendet.
vRealize Log Insight-Appliance	Jede beliebige virtuelle vRealize Log Insight-Appliance (Master oder Worker), auf der sich die vRealize Log Insight-Dienste befinden. Das Basisbetriebssystem der Appliance ist SUSE 11 SP3.

Erforderliche Ports für Daten sendende Quellen

Die folgenden Ports müssen geöffnet sein, um Netzwerkdatenverkehr aus Quellen, die Daten an vRealize Log Insight senden, zu ermöglichen, sowohl für Verbindungen von außerhalb des Clusters als auch für Verbindungen zum Lastenausgleich zwischen Clusterknoten.

Quelle	Ziel	Port	Protokoll	Dienstbeschreibung
Protokolle sendendes System	vRealize Log Insight-Appliance	514	TCP, UDP	Als Weiterleitungsziel konfigurierter ausgehender Syslog-Datenverkehr
Protokolle sendendes System	vRealize Log Insight-Appliance	1514, 6514	TCP	Syslog-Daten über SSL
vRealize Log Insight-Agenten	vRealize Log Insight-Appliance	9000	TCP	Log Insight Ingestion-API
vRealize Log Insight-Agenten	vRealize Log Insight-Appliance	9543	TCP	Ingestion-API von Log Insight über SSL

Erforderliche Ports für die Benutzeroberfläche

Die folgenden Ports müssen geöffnet sein, um Netzwerkdatenverkehr über die vRealize Log Insight-Benutzeroberfläche zu ermöglichen, sowohl für Verbindungen außerhalb des Clusters als auch für Verbindungen zum Lastenausgleich zwischen Clusterknoten.

Quelle	Ziel	Port	Protokoll	Dienstbeschreibung
Admin-Workstation	vRealize Log Insight-Appliance	22	TCP	SSH: Secure Shell-Konnektivität
Benutzer-Workstation	vRealize Log Insight-Appliance	80	TCP	HTTP: Web-Oberfläche
Benutzer-Workstation	vRealize Log Insight-Appliance	443	TCP	HTTPS: Web-Oberfläche

Erforderliche Ports zwischen Clusterknoten

Um maximale Sicherheit zu gewährleisten, sollten die folgenden Ports ausschließlich an einem vRealize Log Insight-Master-Knoten für den Netzwerkzugriff von Worker-Knoten aus geöffnet sein. Diese Ports werden zusätzlich zu den Ports zum Lastenausgleich zwischen Clusterknoten für Quellen und den Datenverkehr über die Benutzeroberfläche geöffnet.

Quelle	Ziel	Port	Protokoll	Dienstbeschreibung
vRealize Log Insight-Appliance	vRealize Log Insight-Appliance	7000	TCP	Cassandra-Replizierung und -Abfrage
vRealize Log Insight-Appliance	vRealize Log Insight-Appliance	9042	TCP	Cassandra-Dienst für native Protokoll-Clients
vRealize Log Insight-Appliance	vRealize Log Insight-Appliance	9160	TCP	Cassandra-Dienst für Thrift-Clients
vRealize Log Insight-Appliance	vRealize Log Insight-Appliance	59778, 16520-16580	TCP	Thrift-Dienst von vRealize Log Insight

Erforderliche Ports für externe Dienste

Die folgenden Ports müssen für ausgehenden Netzwerkdatenverkehr von vRealize Log Insight-Clusterknoten zu Remotediensten geöffnet sein.

Quelle	Ziel	Port	Protokoll	Dienstbeschreibung
vRealize Log Insight-Appliance	NTP-Server	123	UDP	NTPD: sorgt für die NTP-Uhrzeitsynchronisierung Hinweis Der Port ist nur dann geöffnet, wenn Sie die NTP-Uhrzeitsynchronisierung verwenden.
vRealize Log Insight-Appliance	Mail-Server	25	TCP	SMTP: Mail-Dienst für ausgehende Warnungen
vRealize Log Insight-Appliance	Mail-Server	465	TCP	SMTPS: Mail-Dienst über SSL für ausgehende Warnungen
vRealize Log Insight-Appliance	DNS Server	53	TCP, UDP	DNS: Namensauflösungsdienst
vRealize Log Insight-Appliance	AD-Server	389	TCP, UDP	Active Directory
vRealize Log Insight-Appliance	AD-Server	636	TCP	Active Directory über SSL
vRealize Log Insight-Appliance	AD-Server	3268	TCP	Globaler Active Directory-Katalog
vRealize Log Insight-Appliance	AD-Server	3269	TCP	SSL für globalen Active Directory-Katalog
vRealize Log Insight-Appliance	AD-Server	88	TCP, UDP	Kerberos
vRealize Log Insight-Appliance	vCenter Server	443	TCP	vCenter Server-Webservice

Quelle	Ziel	Port	Protokoll	Dienstbeschreibung
vRealize Log Insight-Appliance	vRealize Operations Manager-Appliance	443	TCP	vRealize Operations-Webservice
vRealize Log Insight-Appliance	Protokollmanager eines Drittanbieters	514	TCP, UDP	Syslog-Daten
vRealize Log Insight-Appliance	Protokollmanager eines Drittanbieters	9000	CFAPI	Als Weiterleitungsziel konfigurierter ausgehender Log Insight-Erfassungs-API(CFAPI)-Datenverkehr
vRealize Log Insight-Appliance	Protokollmanager eines Drittanbieters	9543	CFAPI	Als Weiterleitungsziel mit Verschlüsselung (SSL/TLS) konfigurierter ausgehender Log Insight-Erfassungs-API(CFAPI)-Datenverkehr

Ports, die blockiert werden können

Die folgenden Ports sind offen, werden von vRealize Log Insight aber nicht verwendet. Diese Ports können auf sichere Weise von einer Firewall blockiert werden.

Ziel	Port	Protokoll	Dienstbeschreibung
vRealize Log Insight-Appliance	111	TCP, UDP	RPCbind-Dienst, der RPC-Programmnummern in universelle Adressen konvertiert
Tomcat-Dienst der vRealize Log Insight-Appliance	9007	TCP	Tomcat-Dienste

Überwachen des Status von vRealize Log Insight Windows- und Linux-Agenten

7

Sie können den Status der Windows- und Linux-Agenten von vRealize Log Insight überwachen und aktuelle Statistiken über deren Betrieb anzeigen.


Nur Agenten, die für das Senden von Daten über CFAPI konfiguriert sind, werden auf der Seite „Agenten“ angezeigt. Agenten, die gemäß ihrer Konfiguration Daten über Syslog senden, werden wie andere Syslog-Quellen auf der Seite „Hosts“ angezeigt.

Hinweis Wenn Sie eine Host-IP-Adresse für einen vRealize Log Insight-Server in der Agentenkonfiguration ändern, setzt der Agent die Seitenstatistiken auf null zurück.

Voraussetzungen

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.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Klicken Sie unter „Verwaltung“ auf **Agenten**.

Weiter

Anhand der Informationen auf der Seite „Agenten“ können Sie den Betrieb der installierten Windows- und Linux-Agenten von vRealize Log Insight überwachen.

Aktivieren der automatischen Agent-Aktualisierung vom Server



Sie können die automatische Aktualisierung für alle Agenten vom vRealize Log Insight-Server aktivieren.


Die automatische Aktualisierung führt das neueste verfügbare Update für alle Agenten aus, die mit dem Server verbunden sind. Sie können die Funktion der automatischen Aktualisierung für einzelne Server deaktivieren, indem Sie die Datei `liagent.ini` des Agenten entsprechend bearbeiten. Weitere Informationen finden Sie unter *Arbeiten mit vRealize Log Insight-Agenten*.

Die automatische Aktualisierung ist für den Server standardmäßig deaktiviert.

Voraussetzungen

Agenten müssen aktiviert und in der Version 4.3 oder höher vorhanden sein.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Klicken Sie im Menü auf der linken Seite auf **Agenten**.
- 3 Klicken Sie auf der Seite „Agenten“ auf die Umschaltfläche **Automatische Aktualisierung für alle Agenten aktivieren**.

Die Agenten, die mit diesem Server verbunden sind, werden aktualisiert, wenn ein Update vorhanden ist.

Arbeiten mit Agentengruppen

Mithilfe von vRealize Log Insight-Server können Sie Agenten über die Benutzeroberfläche der Anwendung konfigurieren. Agenten fragen den vRealize Log Insight-Server regelmäßig ab, um zu ermitteln, ob neue Konfigurationen verfügbar sind.

Sie können Agenten, für die dieselbe Konfiguration erforderlich ist, in Gruppen zusammenfassen. Zum Beispiel können Sie alle vRealize Log Insight-Windows-Agenten getrennt von den vRealize Log Insight-Linux-Agenten in Gruppen zusammenfassen.

Im Menü **Alle Agenten** werden vorhandene Agentengruppen von Inhaltspaketen automatisch aufgeführt. Die aufgeführten Agenten sind mit von Ihnen schon installierten Inhaltspaketen verknüpft (zum Beispiel das vSphere-Inhaltspaket), die Agentengruppen verwenden.

Inhaltspaketgruppen sind schreibgeschützt.

Nur Konfigurationsabschnitte, die mit [winlog], [filelog] und [parser] beginnen, werden in Inhaltspaketen verwendet. Zusätzliche Abschnitte werden nicht als Bestandteil eines Inhaltspakets exportiert. Nur einzeilige Kommentare (Zeilen, die mit ; beginnen) in den Abschnitten [winlog], [filelog] und [parser] bleiben in einem Inhaltspaket erhalten.

In *Arbeiten mit vRealize Log Insight-Agenten* finden Sie Informationen zum Konfigurieren von Agenten, einschließlich Informationen zum Zusammenführen von Konfigurationen zwischen lokalen und serverseitigen Konfigurationen.

- [Zusammenführen von Agentengruppen-Konfigurationen](#)

Mit Agentengruppen können Agenten Teil von mehreren Gruppen sein und der Standardgruppe *Alle Agenten* angehören, was eine zentrale Konfiguration ermöglicht.

- [Erstellen einer Agentengruppe](#)

Sie können eine Gruppe von Agenten erstellen, die mit denselben Parametern konfiguriert werden.

- [Bearbeiten einer Agentengruppe](#)

Sie können den Namen und die Beschreibung einer Agentengruppe bearbeiten, die Filter ändern und die Konfiguration bearbeiten.

- [Hinzufügen einer Inhaltspaket-Agentengruppe als Agentengruppe](#)

Sie können Ihren aktiven Gruppen eine Agentengruppe hinzufügen, die als Teil eines Inhaltspakets definiert wurde, und auf die Gruppe eine Agentenkonfiguration anwenden.

■ Löschen einer Agentengruppe

Sie können eine Agentengruppe löschen, um sie aus der Liste der aktiven Gruppen zu entfernen.

Zusammenführen von Agentengruppen-Konfigurationen

Mit Agentengruppen können Agenten Teil von mehreren Gruppen sein und der Standardgruppe *Alle Agenten* angehören, was eine zentrale Konfiguration ermöglicht.

Das Zusammenführen erfolgt serverseitig, die sich ergebende Konfiguration wird mit der agentenseitigen Konfiguration zusammengeführt. Die zusammengeführte Konfiguration ergibt sich aus den folgenden Regeln.

- Die einzelnen Gruppenkonfigurationen haben eine höhere Priorität und Vorrang vor den Gruppeneinstellungen „Alle Agenten“.
- Die Gruppenkonfiguration „Alle Agenten“ hat Vorrang vor der lokalen Konfiguration.
- Mit Ausnahme der Gruppe „Alle Agenten“ können Sie keine Abschnitte mit demselben Namen in verschiedenen Gruppen konfigurieren. Die Abschnitte in den einzelnen Gruppen haben jedoch eine höhere Priorität.

Hinweis Um den Verlust von Agenten zu verhindern, können die Parameter **hostname** und **port** einer Agent-Konfiguration nicht zentral vom Server aus geändert werden.

Die zusammengeführte Konfiguration wird in der agentenseitigen Datei `liagent-effective.ini` gespeichert.


Erstellen einer Agentengruppe

Sie können eine Gruppe von Agenten erstellen, die mit denselben Parametern konfiguriert werden.

Voraussetzungen

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.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Klicken Sie unter „Verwaltung“ auf **Agenten**.
- 3 Klicken Sie im Menü **Alle Agenten** auf **Neue Gruppe**.
- 4 Geben Sie einen eindeutigen Namen und eine Beschreibung für die Agentengruppe an und klicken Sie auf **Neue Gruppe**.

Die Agentengruppe wird erstellt und in der Liste **Alle Agenten** eingeblendet, sie wird aber nicht gespeichert.

- 5 Legen Sie einen oder mehrere der folgenden Filter für die Agentengruppe fest.

Filter können Platzhalter wie „*“ und „?“ enthalten.

- IP-Adresse
- Hostname
- Version
- Betriebssystem

Sie können zum Beispiel den Betriebssystemfilter `contains` auswählen und den Wert `windows` zum Kennzeichnen aller Ihrer Windows-Agenten für die Konfiguration festlegen.

- 6 Legen Sie die Agentenkonfigurationswerte im Bereich „Agentenkonfiguration“ fest und klicken Sie auf **Neue Gruppe speichern**.

Die Agentenkonfiguration wird nach dem nächsten Abfrageintervall angewendet.


Bearbeiten einer Agentengruppe

Sie können den Namen und die Beschreibung einer Agentengruppe bearbeiten, die Filter ändern und die Konfiguration bearbeiten.

Voraussetzungen

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.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Klicken Sie unter „Verwaltung“ auf **Agenten**.
- 3 Wählen Sie im Menü **Alle Agenten** den Namen der entsprechenden Agentengruppe aus und klicken Sie auf das Bleistiftsymbol, um sie zu bearbeiten.
- 4 Nehmen Sie die gewünschten Änderungen vor.

Zu bearbeitende Option	Aktion
Name oder Beschreibung	Nehmen Sie die erforderlichen Änderungen vor und klicken Sie auf Speichern .
Filter oder Konfiguration	Nehmen Sie die erforderlichen Änderungen vor und klicken Sie auf Gruppe speichern .


Hinzufügen einer Inhaltspaket-Agentengruppe als Agentengruppe

Sie können Ihren aktiven Gruppen eine Agentengruppe hinzufügen, die als Teil eines Inhaltspakets definiert wurde, und auf die Gruppe eine Agentenkonfiguration anwenden.

Voraussetzungen

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.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Klicken Sie unter „Verwaltung“ auf **Agenten**.
- 3 Wählen Sie im Menü **Alle Agenten** eine Agentenvorlage für die Liste „Verfügbare Vorlagen“ aus.
- 4 Klicken Sie auf **Vorlage kopieren** zum Kopieren der Inhaltspaket-Agentengruppe in Ihre aktiven Gruppen.
- 5 Klicken Sie auf **Kopieren**.
- 6 Wählen Sie die erforderlichen Filter aus und klicken Sie auf **Neue Gruppe speichern**.

Die Inhaltspaket-Agentengruppe wird den aktiven Gruppen hinzugefügt und die Agenten werden entsprechend den von Ihnen angegebenen Filtern konfiguriert.


Löschen einer AgentengruppeLöschen einer Agentengruppe

Sie können eine Agentengruppe löschen, um sie aus der Liste der aktiven Gruppen zu entfernen.

Voraussetzungen

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.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Klicken Sie unter „Verwaltung“ auf **Agenten**.
- 3 Wählen Sie im Menü **Alle Agenten** den Namen der zu löschenden Agentengruppe durch Klicken auf das Symbol X neben ihrem Namen aus.
- 4 Klicken Sie auf **Löschen**.

Die Agentengruppe wird aus der Liste der aktiven Gruppen entfernt.

Konfigurieren und Verwenden von vRealize Log Insight Importer

10

Bei vRealize Log Insight Importer handelt es sich um ein Befehlszeilendienstprogramm, das zum Importieren der Offline-Protokolle von Verlaufsdaten aus lokalen Geräten zum vRealize Log Insight-Server verwendet wird.

vRealize Log Insight ist ein Echtzeit-Tool zur Protokollanalyse, mit dem Syslog- oder Agent-Ereignisse in vRealize Log Insight gestreamt werden. In bestimmten Fällen kann der Import früher erfasster Protokolle nötig sein. Mithilfe von vRealize Log Insight Importer können Sie Support-Pakete und archivierte Protokolle in aufgenommene Daten importieren, die über einen bestimmten Zeitraum hinweg erfasst wurden. Sie können Protokolle von Support-Paketen von vRealize Log Insight oder jedem anderen VMware-Produkt analysieren.

vRealize Log Insight Importer enthält die im Folgenden aufgeführten Funktionen.

- vRealize Log Insight Importer sendet Daten über die Ingestion-API.
- Die „filelog“-Erfassung einschließlich der rekursiven Verzeichniserfassung wird unterstützt.
- Importer ist in der Lage, Daten aus ZIP-, TAR- und GZ-Archivdateien zu lesen.
- Sie haben die Möglichkeit, die Daten anzugeben, die rekursiv aus einem verschachtelten Archiv gelesen werden (wie z. B. eine verschachtelte ZIP-Datei) oder ein Verzeichnis in einem Archiv festzulegen.
- 7-Zip wird nicht unterstützt.

Verwenden von vRealize Log Insight Importer

Stellen Sie sicher, dass vRealize Log Insight über einen Zugriff auf den NFS-Server verfügt, auf dem die archivierten Daten gespeichert sind. Wenn aufgrund eines Netzerkausfalls oder Fehlers auf dem NFS-Server der Zugriff auf den NFS-Server nicht möglich ist, kann der Import von archivierten Daten fehlschlagen. Beachten Sie die im Folgenden aufgeführten Einschränkungen für die Anwendung von vRealize Log Insight Importer.

Wenn im Rahmen der Erfassung Protokolle aus einem Paket extrahiert werden, wird automatisch ein Name für das Protokollpaket festgelegt und als Paket-Tag allen extrahierten Protokollen hinzugefügt. Der Tag-Name ist entweder der Dateiname des Protokolls oder bei Verzeichnisquellen der Name des Verzeichnisses. Paket-Tags unterscheiden Pakete auf einem vRealize Log Insight-Server.

Dieses Tag überschreibt alle Tags mit demselben Namen, die in der Manifestdatei angegeben sind. Das Tag kann von Befehlszeilen-Tags, die denselben Namen verwenden, überschrieben werden.

Es gelten die im Folgenden aufgeführten Einschränkungen:

- vRealize Log Insight Importer überprüft nicht den verfügbaren Festplattenspeicher in der virtuellen vRealize Log Insight-Appliance. Deshalb schlägt der Import von archivierten Protokollen möglicherweise fehl, wenn für die virtuelle Appliance nicht ausreichend Speicherplatz verfügbar ist.
- Beim Import von Protokollen werden von vRealize Log Insight keine Fortschrittsinformationen dargestellt. Während der Import von archivierten Daten durchgeführt wird, können Sie anhand der Konsolenausgabe nicht ableiten, wie viel Zeit übrigbleibt, bis der Importvorgang abgeschlossen wird, oder wie groß die bereits importierte Datenmenge ist.

Unterstützte Betriebssysteme

vRealize Log Insight Importer wird bei folgenden Betriebssystemen unterstützt:

- Windows 32-Bit und 64-Bit
- Linux 32-Bit und 64-Bit

Die Linux-Version kann nicht auf einem Apple Macintosh-System ausgeführt werden.

Dieses Kapitel behandelt die folgenden Themen:

- [Informationen zur vRealize Log Insight Importer-Manifestdatei](#)
- [Installieren, Konfigurieren und Ausführen von vRealize Log Insight Importer](#)
- [Beispiele für die Konfiguration von vRealize Log Insight Importer-Manifestdateien](#)
- [vRealize Log Insight Importer-Konfigurationsparameter](#)

Informationen zur vRealize Log Insight Importer - Manifestdatei

vRealize Log Insight Importer verwendet eine Manifestkonfigurationsdatei, um das Protokollformat zu bestimmen und den Speicherort der zu importierenden Daten anzugeben. Die Manifestdatei hat dasselbe Format wie die Konfigurationsdatei `liagent.ini` und weist eine ähnliche Struktur auf.

Sie können Ihre eigenen Manifestdateien erstellen, um beliebige Protokolldateien zu importieren. Obwohl das Erstellen einer Manifestdatei optional ist, müssen Sie nicht den absoluten Pfad zu den Datendateien kennen, sofern Sie eine Manifestdatei verwenden.

Wenn Sie keine Manifestdatei erstellen, verwendet vRealize Log Insight Importer das Standardmanifest, das alle Dateien des Formats `.txt` und `.log` (`include=*.log*;*.txt*`) erfasst und den Auto-Parser (extrahiert Zeitstempel und Schlüssel/Wert-Paar) auf die extrahierten Protokolle anwendet.

Wenn die Konfigurationsdatei `liagent.ini` als Manifestdatei verwendet wird, extrahiert vRealize Log Insight Importer nur die Abschnitte `[filelog]` als Manifest. Alle Optionen für den Abschnitt `[filelog]` werden in vRealize Log Insight Importer unterstützt.

Weitere im Abschnitt [filelog] unterstützte Optionen sowie Konfigurationsbeispiele finden Sie in der Dokumentation zu vRealize Log Insight-Agenten im *vRealize Log Insight Agent-Administratorhandbuch*.

Erstellen einer Manifestdatei

Sie können den Inhalt der Agentenkonfigurationsdatei kopieren und in eine neue TXT-Datei einfügen. Entfernen Sie zum Ermitteln eines dynamischen Pfads den Schrägstrich am Anfang vor dem Verzeichnispfad.

Angeben des Verzeichnispfads

Das im Abschnitt [filelog] angegebene Verzeichnis kann entweder relativ zur Quelle oder absolut sein. Fügen Sie zum Angeben des Verzeichnispfads unter Linux nicht den Schrägstrich am Anfang ein, da vRealize Log Insight Importer den Pfad ansonsten als absolut behandelt.

Um Namensmuster im Wert des Verzeichnisschlüssels anzugeben, können Sie die Zeichen * und ** verwenden.

- Verwenden Sie * als Platzhalter für ein einzelnes Verzeichnis. Verwenden Sie dieses, um auf eine Verschachtelungsebene mit einem beliebigen Ordner hinzuweisen. Beispielsweise können Sie `directory = log_folder_*` verwenden, um alle mit der Zeichenfolge `log_folder_` beginnende Ordner anzuzeigen.
- Verwenden Sie **, um auf eine beliebige Verschachtelungsebene mit einem Ordner hinzuweisen. Sie können z. B. `directory = **/log` verwenden, um einen Ordner mit dem Namen `log` auf einer beliebigen Verschachtelungsebene innerhalb des Quellverzeichnisses anzugeben.

Installieren, Konfigurieren und Ausführen von vRealize Log Insight Importer

Sie können vRealize Log Insight Importer auf Windows oder Linux installieren. Sie können den vRealize Log Insight Importer auch auf einem vRealize Log Insight-Server installieren und über den Server ausführen.

Voraussetzungen

- Stellen Sie sicher, dass Sie auf die [VMware-Download](#)-Website zugreifen können, um den vRealize Log Insight Importer herunterzuladen.
- Schlagen Sie unter [Informationen zur vRealize Log Insight Importer-Manifestdatei](#) nach und erstellen Sie eine Manifestdatei, die Sie mit dem Importfunktion-Dienstprogramm verwenden. Weitere Informationen finden Sie unter [Beispiele für die Konfiguration von vRealize Log Insight Importer-Manifestdateien](#).
- Überprüfen Sie die [vRealize Log Insight Importer-Konfigurationsparameter](#), um die erforderlichen und optional verfügbaren Parameter zu ermitteln.
- Stellen Sie bei der Verwendung des Parameters `honor_timestamp` sicher, dass Sie über die entsprechenden Anmeldedaten verfügen.

- Wenn Sie ein Support-Paket importieren, müssen Sie den Parameter `honor_timestamp` sowie den Benutzernamen und das Kennwort konfigurieren.

Vorgehensweise

- 1 Laden Sie das Installationspaket für vRealize Log Insight Importer von der [VMware-Download-Website](#) herunter und installieren Sie das Tool auf Ihrem System. Das Installationspaket enthält das MSI-Installationsprogramm für Windows und POSIX-Installationspakete (RPM, DEB und BIN) für Linux.

Das vRealize Log Insight Importer-Tool wird an den folgenden Speicherorten installiert:

Betriebssystem	Dateiname	Speicherort der Installation
Windows	loginsight-importer.exe	C:\Programme (x86)\VMware\Log Insight Importer
Linux	loginsight-importer	/usr/lib/loginsight-importer

Hinweis

- Nach der Installation wird auf Windows das Importer-Installationsverzeichnis zur Umgebungsvariable „PATH“ hinzugefügt, und auf Linux wird ein symbolischer Link zur ausführbaren Datei `loginsight-importer` zu `/usr/bin/` hinzugefügt. Dadurch kann der Client `loginsight-importer` von der Shell aus aufrufen, ohne dafür das Präfix eines Pfads angeben zu müssen.
 - Bei der Installation von vRealize Log Insight Importer werden auch eine Reihe von Manifestdateien für VMware-Produkte installiert. Sie können diese Dateien bei der Ausführung von vRealize Log Insight Importer verwenden oder für Ihre Bedürfnisse modifizieren. Die Manifestdateien befinden sich in Windows unter `C:\Program Files (x86)\VMware\Log Insight Importer\Manifests` und in Linux unter `/usr/lib/loginsight-importer/manifests`.
 - Wenn Sie das Paket `.bin` deinstallieren, müssen Sie auch den symbolischen Link `/usr/bin/loginsight_importer` löschen.
- 2 Starten Sie das Tool vRealize Log Insight Importer, indem Sie den folgenden Befehl in eine Eingabeaufforderung eingeben.

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

- 3 Geben Sie an der Eingabeaufforderung den Namen der Manifestdatei ein.
- 4 Legen Sie die Konfigurationsparameter fest und drücken Sie die **Eingabetaste**.

vRealize Log Insight Importer beginnt mit der Extraktion der Protokolleinträge aus den in den Parametern angegebenen Verzeichnissen. Es werden die Gesamtanzahl der verarbeiteten Dateien, der extrahierten Protokollmeldungen, der gesendeten Protokollmeldungen sowie die Laufzeit angezeigt.

- 5 Drücken Sie nach Abschluss des Importvorgangs unter Windows oder Linux **Strg + C**, um das Tool zu beenden.

Weiter

Über die Registerkarte „Interaktive Analyse“ in vRealize Log Insight können Sie die Ansicht für die Auflistung der importierten Protokollereignisse aktualisieren. Wenn Sie ein Support-Paket importiert und den Parameter `honor_timestamp` verwendet haben, sollte das Dashboard auch die Ereignisse im Zeitverlauf anzeigen.

Beispiele für die Konfiguration von vRealize Log Insight Importer -Manifestdateien

Die Beispiele für vRealize Log Insight Importer-Manifestdateien dienen als Beispiele für die Konfiguration von Parametern.

Der Wert des Verzeichnisschlüssels sollte entweder relativ zur Quelle oder absolut sein. Im folgenden Beispiel wird dargestellt, wie Protokolle aus Dateien mit einer `.log`-Erweiterung erfasst werden, welche sich zwei Ebenen unter dem Quellverzeichnis befinden, und bei denen der Name des letzten Ordners mit der Zeichenfolge `_log` endet.

```
[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
```

Im folgenden Beispiel wird dargestellt, wie alle Dateien mit der `.log`-Erweiterung aus allen Unterordnern des Quellverzeichnisses einschließlich der Quelle selbst erfasst werden.

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

Im folgenden Beispiel wird dargestellt, wie Protokolle aus allen Dateien im Quellverzeichnis (nicht jedoch aus den Unterordnern) erfasst werden, ausgenommen die Dateien, die über eine `.ini`-Erweiterung verfügen. Dateien werden als UTF-16LE-codiert interpretiert.

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

Im folgenden Beispiel wird dargestellt, wie Protokolle aus allen Dateien mit der Erweiterung `.log` im Quellverzeichnis (nicht jedoch aus den Unterordnern) erfasst werden. Der Zeitstempel der Ereignisse wird in der Protokolldatei unter Verwendung des Parser im Common Log Format (CLF-Parser) analysiert, und es wird der extrahierte Verlaufszeitstempel angewendet. Das mit dem CLF-Parser analysierte Protokollformat lautet `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
```

vRealize Log Insight Importer -Konfigurationsparameter

Die vRealize Log Insight Importer-Konfiguration umfasst erforderliche und optionale Parameter.

Erforderliche Parameter	Beschreibung
<code>--source <path></code>	Gibt den Pfad zum Verzeichnis des Support-Pakets oder den Pfad zum ZIP-, GZIP- oder TAR-Archiv des Pakets an. Der Wert wird zu allen gesendeten Nachrichten als Wert des <code>bundle</code> -Tags hinzugefügt.
<code>--server <hostname></code>	Hostname oder IP-Adresse des Zielservers.
Optionen	Beschreibung
<code>--port <port></code>	Port für die Verbindung. Wenn kein Wert angegeben ist, wird Port 9000 für Verbindungen ohne SSL und Port 9543 für SSL-Verbindungen verwendet.
<code>--logdir <path></code>	Gibt den Pfad zum Protokollverzeichnis an. Wenn dafür kein Wert angegeben ist, lautet der Pfad für Windows <code>\$(LOCALAPPDATA)\VMware\Log Insight Importer\log</code> und für Linux <code>~/loginsight-importer/log</code> .
<code>--manifest <file-path></code>	Gibt den Pfad zur Manifestdatei an (INI-Format). Wenn dafür kein Wert angegeben ist, wird die Datei <code>importer.ini</code> im Quellverzeichnis verwendet. Wenn die Datei <code>importer.ini</code> im Quellverzeichnis nicht vorhanden ist oder nicht gefunden werden kann, wendet vRealize Log Insight Importer das (hartcodierte) Standard-Manifest an und erfasst alle Dateien des Formats <code>.txt</code> und <code>.log</code> (<code>include=*.log*;*.txt*</code>), und wendet zudem den Auto-Parser an (extrahiert Zeitstempel und Schlüssel/Wert-Paar).
<code>--no_ssl</code>	Verwenden Sie SSL nicht für Verbindungen. Dieser Wert sollte nicht für authentifizierte Verbindungen festgelegt werden (wenn z. B. <code>--honor_timestamp</code> verwendet wird).
<code>--ssl_ca_path <path></code>	Pfad zur Paketdatei der vertrauenswürdigen Stammzertifikate.

Optionen	Beschreibung
<code>--tags <tags></code>	<p>Legen Sie Tags für alle gesendeten Ereignisse fest. Beispiel: <code>--tags "{ \"tag1\" : \"value1\", \"tag2\":\"value2\"}"</code></p> <p>Hinweis Die Tags-Option kann hostname als Tagname akzeptieren. Als Wert für das hostname-Feld für alle durch vRealize Log Insight Importer extrahierten Ereignisse wird der Wert des hostname-Tags aus der Befehlszeile anstelle des FQDN der sendenden Maschine verwendet. Dies ist das Gegenteil von Tags-Parametern in der Manifestdatei und durch Parser extrahierte Felder, welche das hostname-Feld ignorieren.</p> <p>Der Name eines Protokollpakets, der entweder ein Dateiname oder bei Verzeichnisquellen ein Verzeichnisname ist, wird automatisch festgelegt und während der Aufnahme als Paket-Tag allen Protokollen hinzugefügt, die aus dem jeweiligen Paket extrahiert wurden. Mit diesem Tag können Sie Pakete auf dem VMware vRealize® Log Insight-Server voneinander unterscheiden. Paket-Tags überschreiben Tags mit demselben Namen aus Manifestdateien. Sie können jedoch durch Befehlszeilen-Tags überschrieben werden, wenn einer namens Paket vorhanden ist.</p>
<code>--username <username ></code>	Benutzername für die Authentifizierung. Erforderlich, wenn <code>--honor_timestamp</code> festgelegt ist.
<code>--password <password></code>	Kennwort für die Authentifizierung. Erforderlich, wenn <code>--honor_timestamp</code> festgelegt ist. Das Benutzername/Kennwort-Paar deaktiviert die zulässige Zeitabweichung auf dem vRealize Log Insight-Server, um das Importieren von Daten mit einem historischen Zeitstempel zu ermöglichen.
<code>--honor_timestamp</code>	<p>Wendet den extrahierten Zeitstempel an. Die konfigurierten Parser extrahieren den Zeitstempel aus den Protokolleinträgen, und <code>--honor_timestamp</code> wendet den extrahierten Zeitstempel an.</p> <ul style="list-style-type: none"> ■ Wenn der Zeitstempel mithilfe von konfigurierten Parsern extrahiert wird, wird dieser Zeitstempel auf Ereignisse angewendet. ■ Wenn sich in der Protokolldatei ein Ereignis ohne extrahierten Zeitstempel befindet, wird der erfolgreich extrahierte Zeitstempel aus dem vorherigen Ereignis in derselben Protokolldatei angewendet. ■ Wenn in der Datei kein Zeitstempel gefunden oder analysiert wird, wird die MTIME der Protokolldatei als Zeitstempel angewendet. <p>Hinweis Wenn keine Manifestdatei bereitgestellt wurde, ist für das hartcodierte Standard-Manifest, das von vRealize Log Insight Importer verwendet wird, der automatische Protokollparser aktiviert. In diesem Fall extrahiert vRealize Log Insight Importer den Zeitstempel aus den Protokolleinträgen, wenn der Parameter <code>--honor_timestamp</code> verwendet wird.</p>
<code>--debug_level <1 2></code>	Erhöht den Ausführlichkeitsgrad der Protokolldatei. Dies sollte nur im Rahmen einer Fehlerbehebung geändert werden. Im Normalbetrieb sollte dieses Flag nicht verwendet werden.
<code>--help</code>	Zeigen Sie Hilfe an und beenden Sie das Programm.

Überwachen von vRealize Log Insight

11

Sie können die virtuelle Appliance von vRealize Log Insight und die Hosts und Geräte überwachen, die Protokollereignisse zu vRealize Log Insight senden.

Dieses Kapitel behandelt die folgenden Themen:

- [Prüfen des Systemzustands der virtuellen vRealize Log Insight-Appliance](#)
- [Überwachen von Protokollereignisse sendenden Hosts](#)


Prüfen des Systemzustands der virtuellen vRealize Log Insight -Appliance

Sie können die verfügbaren Ressourcen und aktiven Abfragen auf der virtuellen vRealize Log Insight-Appliance überprüfen und aktuelle Statistiken über den Betrieb von vRealize Log Insight aufrufen.

Voraussetzungen

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.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Management, click **System Monitor**.
- 3 Wenn vRealize Log Insight als Cluster ausgeführt wird, klicken Sie auf **Ressourcen anzeigen für** und wählen Sie den Knoten aus, den Sie überwachen möchten.

- 4 Klicken Sie auf die Schaltflächen auf der Seite „Systemüberwachung“, um die benötigten Informationen anzuzeigen.

Option	Beschreibung
Ressourcen	Anzeigen von Informationen über CPU, Arbeitsspeicher, IOPS (Lese- und Schreibvorgänge) und Speichernutzung auf der virtuellen vRealize Log Insight-Appliance. Die Diagramme auf der rechten Seite zeigen historische Daten der letzten 24 Stunden und werden alle fünf Minuten aktualisiert. Die Diagramme auf der linken Anzeige enthalten Informationen der letzten fünf Minuten und werden alle drei Sekunden aktualisiert.
Aktive Abfragen	Anzeigen von Informationen zu den derzeit in vRealize Log Insight aktiven Abfragen.
Statistiken	Anzeigen von Statistiken zu den Protokollaufnahmevergängen und -raten. Um detaillierte Statistiken anzuzeigen, klicken Sie auf Erweiterte Statistik anzeigen .

Weiter

Sie können mit den Informationen der Seite „Systemüberwachung“ Ressourcen auf der virtuellen vRealize Log Insight-Appliance verwalten.

Überwachen von Protokollereignisse sendenden Hosts


Sie können eine Liste mit allen Hosts und Geräten anzeigen, die Protokollereignisse an vRealize Log Insight senden, um diese zu überwachen.

Einträge in Hosttabellen werden drei Monate nach dem letzten erfassten Ereignis ungültig.

Voraussetzungen

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.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Klicken Sie unter „Verwaltung“ auf **Hosts**.

Hinweis Wenn Sie einen vCenter Server zum Senden von Ereignissen und Warnungen konfiguriert haben, die einzelnen ESXi-Hosts jedoch nicht zum Senden von Protokollen konfiguriert haben, werden in der Liste „Hostname“ nicht nur die vCenter Server-Hosts, sondern auch die einzelnen ESXi-Hosts als Quelle aufgelistet.

Integration von vRealize Log Insight in VMware-Produkte

12

vRealize Log Insight kann in andere VMware-Produkte eingebunden werden, um Ereignisse und Protokolldaten zu verwenden und eine bessere Einsicht in Ereignisse zu bieten, die in einer virtuellen Umgebung auftreten.

Integration in VMware vSphere

vRealize Log Insight-Administratorbenutzer können vRealize Log Insight so einrichten, dass alle zwei Minuten eine Verbindung mit vCenter Server hergestellt wird und Ereignis-, Warnungs- und Aufgabendaten dieser vCenter Server-Systeme gesammelt werden. Außerdem kann vRealize Log Insight ESXi-Hosts über vCenter Server konfigurieren. Weitere Informationen hierzu finden Sie unter [Verbinden von vRealize Log Insight mit einer vSphere-Umgebung](#).

Integration in VMware vRealize Operations Manager

Sie können vRealize Log Insight in vRealize Operations Manager vApp und vRealize Operations Manager Installable integrieren. Die Integration in die Installable-Version erfordert zusätzliche Änderungen an der Konfiguration von vRealize Operations Manager. Informationen zur Konfiguration von vRealize Operations Manager Installable zur Integration in vRealize Log Insight finden Sie in der Anleitung *Erste Schritte für Log Insight*.

vRealize Log Insight und vRealize Operations Manager lassen sich auf zwei unabhängige Weisen integrieren.

Benachrichtigungsereignisse

vRealize Log Insight-Administratorbenutzer können vRealize Log Insight so einrichten, dass auf von Ihnen erstellten Abfragen basierende Benachrichtigungsereignisse an vRealize Operations Manager gesendet werden. Weitere Informationen hierzu finden Sie unter [Konfigurieren von vRealize Log Insight zum Senden von Benachrichtigungsereignissen an vRealize Operations Manager](#).

Kontextbezogener Start

Kontextbezogener Start ist eine Funktion in vRealize Operations Manager, die es Ihnen ermöglicht, in einem bestimmten Kontext eine externe Anwendung per URL zu starten. Der Kontext wird durch das aktive Benutzeroberflächenelement und die Objektauswahl definiert. Über den kontextbezogenen Start kann der vRealize Log Insight-Adapter einer Reihe

verschiedener Ansichten innerhalb der benutzerdefinierten Benutzeroberfläche und der vSphere-Benutzeroberfläche von vRealize Operations Manager Menüelemente hinzufügen. Weitere Informationen hierzu finden Sie unter [Aktivieren des kontextbezogenen Starts für vRealize Log Insight in vRealize Operations Manager](#).

Hinweis Benachrichtigungsereignisse hängen nicht von der Konfiguration des kontextbezogenen Starts ab. Sie können Benachrichtigungsereignisse auch dann von vRealize Log Insight an vRealize Operations Manager senden, wenn Sie die Funktion Kontextbezogener Start nicht aktivieren.

Wenn sich die Umgebung verändert, können Administratorbenutzer von vRealize Log Insight vSphere-Systeme ändern, hinzufügen oder aus vRealize Log Insight entfernen, die vRealize Operations Manager-Instanz ändern oder entfernen, an die Warnungsbenachrichtigungen gesendet werden, und die zur Verbindung von vSphere-Systemen und vRealize Operations Manager verwendeten Kennwörter ändern.

Dieses Kapitel behandelt die folgenden Themen:

- [Verbinden von vRealize Log Insight mit einer vSphere-Umgebung](#)
- [Konfigurieren von vRealize Log Insight für das Abrufen von Ereignissen, Aufgaben und Warnungen aus vCenter Server-Instanzen](#)
- [Verwenden von vRealize Operations Manager mit vRealize Log Insight](#)
- [vRealize Operations Manager-Inhaltspaket für vRealize Log Insight](#)

Verbinden von vRealize Log Insight mit einer vSphere-Umgebung

Bevor Sie vRealize Log Insight für die Erfassung von Warnungs-, Ereignis- und Aufgabendaten aus Ihrer vSphere-Umgebung konfigurieren, müssen Sie vRealize Log Insight mit einem oder mehreren vCenter Server-Systemen verbinden.

vRealize Log Insight kann zwei Arten von Daten aus vCenter Server-Instanzen und den ESXi-Hosts, die sie verwalten, erfassen.

- Ereignisse, Aufgaben und Warnungen sind strukturierte Daten mit spezifischer Bedeutung. Nach erfolgter Konfiguration ruft vRealize Log Insight Ereignisse, Aufgaben und Warnungen der registrierten vCenter Server-Instanzen ab.
- Protokolle enthalten unstrukturierte Daten, die in vRealize Log Insight analysiert werden können. ESXi-Hosts oder vCenter Server Appliance-Instanzen können ihre Protokolle über Syslog an vRealize Log Insight übermitteln.

Voraussetzungen


- Vergewissern Sie sich, dass Sie für den gewünschten Integrationsgrad über Anmeldedaten mit ausreichenden Rechten verfügen, um die erforderliche Konfiguration am vCenter Server-System und dessen ESXi-Hosts vorzunehmen.

Integrationsgrad	Erforderliche Berechtigungen
Erfassung von Ereignissen, Aufgaben und Alarmen	<ul style="list-style-type: none"> ■ System.Anzeigen <p>Hinweis System.Anzeigen ist eine systemdefinierte Berechtigung. Wenn Sie eine benutzerdefinierte Rolle hinzufügen, ohne ihr Berechtigungen zuzuweisen, wird sie als schreibgeschützte Rolle mit drei systemdefinierten Berechtigungen erstellt: System.Anonym, System.Anzeigen und System.Lesen.</p>
Syslog-Konfiguration auf ESXi-Hosts	<ul style="list-style-type: none"> ■ Host.Konfiguration.Einstellungen ändern ■ Host.Konfiguration.Netzwerkconfiguration ■ Host.Konfiguration.Erweiterte Einstellungen ■ Host.Konfiguration.Sicherheitsprofil und Firewall

Hinweis Sie müssen die Berechtigung für die Ordner der obersten Ebene in der vCenter Server-Bestandsliste konfigurieren und sicherstellen, dass das Kontrollkästchen **An untergeordnete Objekte weitergeben** markiert ist.

- Sie müssen die IP-Adresse oder den Domännennamen des vCenter Server-Systems kennen.
- 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.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Klicken Sie unter „Integration“ auf **vSphere**.
- 3 Geben Sie die IP-Adresse und die Anmeldedaten für einen vCenter Server ein und klicken Sie auf **Verbindung testen**.

Die Verwendung von Anmeldedaten für das Dienstkonto wird empfohlen.

- 4 (Optional) Klicken Sie, um einen weiteren vCenter Server zu registrieren, auf **vCenter Server hinzufügen** und wiederholen Sie die Schritte 3 bis 5.

Hinweis Registrieren Sie keine vCenter Server-Systeme mit doppelt vorhandenen Namen oder IP-Adressen. vRealize Log Insight prüft nicht, ob vCenter Server-Namen doppelt vorhanden sind. Sie müssen sicherstellen, dass die Liste der registrierten vCenter Server-Systeme keine doppelten Einträge enthält.

- 5 Click **Save**.

Weiter

- Starten Sie die Erfassung von Ereignis-, Aufgaben- und Warnungsdaten aus der vCenter Server-Instanz, die Sie registriert haben. Weitere Informationen hierzu finden Sie unter [Konfigurieren von vRealize Log Insight für das Abrufen von Ereignissen, Aufgaben und Warnungen aus vCenter Server-Instanzen](#).
- Starten Sie die Erfassung von Syslog-Feeds von den durch vCenter Server verwalteten ESXi-Hosts. Weitere Informationen hierzu finden Sie unter [Konfigurieren eines ESXi-Hosts für die Weiterleitung von Protokollereignissen an vRealize Log Insight](#).

vRealize Log Insight als Syslog-Server

vRealize Log Insight umfasst einen integrierten Syslog-Server, der während der Ausführung des vRealize Log Insight-Diensts andauernd aktiv ist.

Der Syslog-Server überwacht die Ports 514/TCP, 1514/TCP und 514/UDP und kann Protokollnachrichten anderer Hosts aufnehmen. Vom Syslog-Server aufgenommene Nachrichten können in der vRealize Log Insight-Web-Benutzeroberfläche nahezu in Echtzeit durchsucht werden. Damit vRealize Log Insight die Syslog-Nachrichten akzeptieren kann, dürfen sie nicht größer als 10 KB sein.

Konfigurieren eines ESXi -Hosts für die Weiterleitung von Protokollereignissen an vRealize Log Insight

ESXi-Hosts und vCenter Server Appliance-Instanzen generieren unstrukturierte Protokolldaten, die in vRealize Log Insight analysiert werden können.

Sie verwenden die Verwaltungsschnittstelle von vRealize Log Insight zum Konfigurieren von ESXi-Hosts auf einem registrierten vCenter Server, um Syslog-Daten zu vRealize Log Insight zu senden.

Vorsicht Das Ausführen paralleler Konfigurationsaufgaben kann möglicherweise zu fehlerhaften Syslog-Einstellungen auf dem ESXi-Zielhost führen. Stellen Sie sicher, dass kein anderer Administrator die ESXi-Hosts konfiguriert, die Sie konfigurieren möchten.

Ein vRealize Log Insight-Cluster kann einen integrierten Lastausgleichsdienst verwenden, um Syslog-Feeds von ESXi und vCenter Server Appliance auf die einzelnen Knoten des Clusters zu verteilen.

Weitere Informationen über das Filtern von Syslog-Nachrichten auf ESXi-Hosts vor dem Senden von Nachrichten an vRealize Log Insight finden Sie unter *Konfigurieren der Protokollfilterung auf ESXi-Hosts* im Abschnitt [Einrichten von ESXi](#) im **Installations- und Einrichtungshandbuch für vSphere**.

Informationen zur Konfiguration von Syslog-Feeds über eine vCenter Server Appliance finden Sie unter [Konfigurieren von vCenter Server für das Weiterleiten von Protokollereignissen an vRealize Log Insight](#).


Hinweis vRealize Log Insight kann Syslog-Daten von ESXi-Hosts der Version 5.5 und höher empfangen.

Voraussetzungen

- Stellen Sie sicher, dass der vCenter Server, der den ESXi-Host verwaltet, bei Ihrer vRealize Log Insight-Instanz registriert ist. Alternativ können Sie in einem Vorgang auch den ESXi-Host registrieren und vCenter Server konfigurieren.
- Vergewissern Sie sich, dass Ihre Anmeldeinformationen über die erforderlichen Rechte zur Konfiguration von Syslog auf ESXi-Hosts verfügen.
 - **Host.Konfiguration.Erweiterte Einstellungen**
 - **Host.Konfiguration.Sicherheitsprofil und Firewall**

Hinweis Sie müssen die Berechtigung für die Ordner der obersten Ebene in der vCenter Server-Bestandsliste konfigurieren und sicherstellen, dass das Kontrollkästchen **An untergeordnete Objekte weitergeben** markiert ist.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Klicken Sie unter „Integration“ auf **vSphere**.
- 3 Suchen Sie die vCenter Server-Instanz, die den ESXi-Host, von dem Sie Syslog-Feeds erhalten möchten, verwaltet.
- 4 Aktivieren Sie das Kontrollkästchen **ESXi-Hosts für das Versenden von Protokollen an Log Insight konfigurieren**.

vRealize Log Insight konfiguriert standardmäßig alle erreichbaren ESXi-Hosts der Version 5.5 und höher so, dass sie ihre Protokolle über UDP senden.

- 5 (Optional) Um die Standardwerte für die Konfiguration zu ändern, klicken Sie auf **Erweiterte Optionen**.
 - Um das Protokoll für alle ESXi-Hosts zu ändern, wählen Sie **Alle ESXi-Hosts konfigurieren** sowie ein Protokoll aus und klicken Sie auf **OK**.
 - Um die Protokollierung für bestimmte ESXi-Hosts einzurichten oder das Protokoll für ausgewählte ESXi-Hosts zu ändern, verwenden Sie die folgenden Schritte:
 - a Wählen Sie **Bestimmte ESXi-Hosts konfigurieren** aus.
 - b Wählen Sie einen oder mehrere Hosts aus der Liste **Nach Host filtern** aus.
 - c Legen Sie den Protokollwert fest.
 - d Klicken Sie auf **OK**.
- 6 (Optional) Wenn Sie Cluster verwenden, öffnen Sie das Dropdown-Menü für das Textfeld **Ziel** und wählen Sie den Hostnamen oder die IP-Adresse für den Lastausgleichsdienst aus, der die Syslog-Feeds verteilt.
- 7 Click **Save**.

Ändern einer ESXi -Hostkonfiguration für die Weiterleitung von Protokollereignissen an vRealize Log Insight

ESXi-Hosts und vCenter Server Appliance-Instanzen generieren unstrukturierte Protokolldaten, die in vRealize Log Insight analysiert werden können.

Sie verwenden die Verwaltungsschnittstelle von vRealize Log Insight zum Konfigurieren von ESXi-Hosts auf einem registrierten vCenter Server, um Syslog-Daten zu vRealize Log Insight zu senden.

Vorsicht Das Ausführen paralleler Konfigurationsaufgaben kann möglicherweise zu fehlerhaften Syslog-Einstellungen auf dem ESXi-Zielhost führen. Stellen Sie sicher, dass kein anderer Administrator die ESXi-Hosts konfiguriert, die Sie konfigurieren möchten.

Nach dem Einrichten der anfänglichen Konfiguration können Sie eine Option aktivieren, um einen ESXi-Host automatisch mit dem Standardprotokoll zu konfigurieren, wenn er zu einem Cluster hinzugefügt wird.

Ein vRealize Log Insight-Cluster kann einen integrierten Lastausgleichsdienst verwenden, um Syslog-Feeds von ESXi und vCenter Server Appliance auf die einzelnen Knoten des Clusters zu verteilen.

Weitere Informationen über das Filtern von Syslog-Nachrichten auf ESXi-Hosts vor dem Senden von konfigurierten Nachrichten an vRealize Log Insight finden Sie unter *Konfigurieren der Protokollfilterung auf ESXi-Hosts* im Abschnitt [Einrichten von ESXi](#) im **Installations- und Einrichtungshandbuch für vSphere**.

Informationen zur Konfiguration von Syslog-Feeds über eine vCenter Server Appliance finden Sie unter [Konfigurieren von vCenter Server für das Weiterleiten von Protokollereignissen an vRealize Log Insight](#).

Hinweis vRealize Log Insight kann Syslog-Daten von ESXi-Hosts der Version 5.5 und höher empfangen.

Voraussetzungen

- Stellen Sie sicher, dass der vCenter Server, der den ESXi-Host verwaltet, bei Ihrer vRealize Log Insight-Instanz registriert ist.
- Vergewissern Sie sich, dass Ihre Anmeldeinformationen über die erforderlichen Rechte zur Konfiguration von Syslog auf ESXi-Hosts verfügen.
 - **Host.Konfiguration.Erweiterte Einstellungen**
 - **Host.Konfiguration.Sicherheitsprofil und Firewall**

Hinweis Sie müssen die Berechtigung für die Ordner der obersten Ebene in der vCenter Server-Bestandsliste konfigurieren und sicherstellen, dass das Kontrollkästchen **An untergeordnete Objekte weitergeben** markiert ist.

Vorgehensweise

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

- 2 Klicken Sie unter „Integration“ auf **vSphere**.
- 3 Aktivieren Sie das Kontrollkästchen **ESXi-Hosts für das Versenden von Protokollen an Log Insight konfigurieren**.
- 4 Klicken Sie auf **Erweiterte Optionen**.
- 5 Um das Protokoll für ausgewählte ESXi-Hosts zu ändern, verwenden Sie die folgenden Schritte:
 - a Wählen Sie einen oder mehrere Hosts aus der Liste **Nach Host filtern** aus.
 - b Legen Sie den Protokollwert fest.
 - c Um auszuwählen, dass ein ESXi-Host automatisch mit dem Standardprotokoll konfiguriert wird, wenn es zu einem vRealize Log Insight-Cluster hinzugefügt wird, wählen Sie **Alle ESXi-Hosts automatisch konfigurieren** aus.
 - d Klicken Sie auf **Konfigurieren**.
- 6 (Optional) Wenn Sie Cluster verwenden, können Sie einen Lastausgleichsdienst angeben, indem Sie das Dropdown-Menü für das Textfeld **Ziel** auf dem Bildschirm **vSphere-Integration** öffnen und den Hostnamen oder die IP-Adresse für den Lastausgleichsdienst auswählen.

vRealize Log Insight -Benachrichtigungsereignisse in vRealize Operations Manager

Sie können vRealize Log Insight konfigurieren, damit Benachrichtigungsereignisse an vRealize Operations Manager auf Basis der von Ihnen erstellten Warnungsabfragen gesendet werden.

Wenn Sie eine Benachrichtigungswarnung in vRealize Log Insight konfigurieren, wählen Sie eine Ressource in vRealize Operations Manager aus, die den Benachrichtigungsereignissen zugeordnet ist. Siehe [Hinzufügen einer Warnungsabfrage in Log Insight, um Benachrichtigungsereignisse an vRealize Operations Manager zu senden](#).

Im Folgenden werden Abschnitte der Benutzeroberfläche von vRealize Operations Manager aufgelistet, in denen Benachrichtigungsereignisse angezeigt werden.

- Startseite > Dashboard **Empfehlungen** > **Top-Systemzustandswarnungen für abgeleitete Elemente**
- Startseite > Registerkarte **Warnungen**
- Auf allen benutzerdefinierten Dashboards, die Widgets mit Benachrichtigungsereignissen enthalten

Weitere Informationen dazu, wo Benachrichtigungsereignisse angezeigt werden, finden Sie im [VMware vRealize Operations Manager-Dokumentationscenter](#).

Konfigurieren von vCenter Server für das Weiterleiten von Protokollereignissen an vRealize Log Insight

Die vSphere-Integration erfasst Aufgaben und Ereignisse von vCenter Server, jedoch nicht die internen Protokolle auf niedriger Ebene für die einzelnen vCenter Server-Komponenten. Diese Protokolle werden vom vSphere-Inhaltspaket genutzt.

Die Konfiguration für vCenter Server 6.5 und höhere Versionen muss über die Verwaltungsschnittstelle der vCenter Server Appliance vorgenommen werden. Weitere Informationen über die Weiterleitung von Protokollereignissen vom vCenter Server finden Sie in der vSphere-Dokumentation zum Thema der Umleitung von Protokolldateien der vCenter Server Appliance auf einen anderen Computer.

Für frühere Versionen von vSphere wird die Installation eines vRealize Log Insight-Agenten empfohlen, obwohl die vCenter Server Appliance einen Syslog-Daemon enthält, der für die Weiterleitung von Protokollen verwendet werden kann.

Weitere Informationen zum Installieren von vRealize Log Insight-Agenten finden Sie im *vRealize Log Insight Agent-Administratorhandbuch* im [vRealize Log Insight-Informationscenter](#).

Das vSphere-Inhaltspaket enthält Agentengruppen, die bestimmte Protokolldateien zur Erfassung von vCenter Server-Installationen definieren. Die Konfiguration wird unter `https://LogInsightServerFqdnOrIP/contentpack?contentPackId=com.vmware.vsphere` gezeigt.

Weitere Informationen zum Arbeiten mit Agentengruppen finden Sie unter [Kapitel 9 Arbeiten mit Agentengruppen](#).

Weitere Informationen zu den Speicherorten für vCenter Server-Protokolldateien finden Sie unter `http://kb.vmware.com/kb/1021804` und `http://kb.vmware.com/kb/1021806`.

Konfigurieren von vRealize Log Insight für das Abrufen von Ereignissen, Aufgaben und Warnungen aus vCenter Server -Instanzen

Ereignisse, Aufgaben und Warnungen sind strukturierte Daten mit spezifischer Bedeutung. Sie können vRealize Log Insight für die Erfassung von Warnungs-, Ereignis- und Aufgabendaten aus einem oder mehreren vCenter Server-Systemen konfigurieren.

Über die Administrations-Benutzeroberfläche können Sie vRealize Log Insight für die Verbindung mit vCenter Server-Systemen konfigurieren. Die Informationen werden von den vCenter Server-Systemen mithilfe der vSphere Web Services-API abgerufen und in der Web-Benutzeroberfläche von vRealize Log Insight als vSphere-Inhaltspaket angezeigt.


Hinweis vRealize Log Insight kann Warnungs-, Ereignis- und Aufgabendaten nur von vCenter Server 5.1 und höher abrufen.

Voraussetzungen

Vergewissern Sie sich, dass Sie über Anmeldedaten mit **System.View**-Berechtigungen verfügen.

Hinweis Sie müssen die Berechtigung für die Ordner der obersten Ebene in der vCenter Server-Bestandsliste konfigurieren und sicherstellen, dass das Kontrollkästchen **An untergeordnete Objekte weitergeben** markiert ist.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Klicken Sie unter „Integration“ auf **vSphere**.
- 3 Suchen Sie die vCenter Server-Instanz, aus der Sie Daten erfassen möchten, und aktivieren Sie das Kontrollkästchen **vCenter Server-Ereignisse, -Aufgaben und -Warnungen sammeln**.
- 4 Click **Save**.

vRealize Log Insight verbindet sich alle zwei Minuten mit vCenter Server und bezieht alle neuen Informationen seit dem letzten Abruf.

Weiter

- Analysieren Sie vSphere-Ereignisse mit dem vSphere-Inhaltspaket oder mittels benutzerdefinierter Abfragen.
- Aktivieren Sie Inhaltspaketwarnungen oder benutzerdefinierte Benachrichtigungen für vSphere.

Verwenden von vRealize Operations Manager mit vRealize Log Insight

Anforderungen für die Integration in vRealize Operations Manager

Zur Integration von vRealize Log Insight in vRealize Operations Manager müssen Anmeldedaten für vRealize Log Insight zur Authentifizierung bei vRealize Operations Manager festgelegt werden. vRealize Operations Manager unterstützt sowohl lokale Benutzerkonten als auch mehrere LDAP-Quellen.

So ermitteln Sie den Benutzernamen für ein lokales Benutzerkonto:

- 1 Öffnen Sie die Web-Benutzeroberfläche von vRealize Operations Manager.
- 2 Wählen Sie **Zugriffssteuerung** aus.
- 3 Identifizieren bzw. erstellen Sie den Integrationsbenutzer. Das Feld für den Quelltyp ist **Lokaler Benutzer**.
- 4 Der Benutzername, der auf der vRealize Log Insight-Benutzeroberfläche für die Administration eingegeben werden sollte, entspricht dem Inhalt des Felds **Benutzername**.

Zur Ermittlung des Benutzernamenformats für das LDAP-Benutzerkonto, das in vRealize Log Insight anzugeben ist, gehen Sie nach diesen Anweisungen vor:

- 1 Öffnen Sie die Web-Benutzeroberfläche von vRealize Operations Manager.
- 2 Wählen Sie „Zugriffssteuerung“ aus.
- 3 Identifizieren bzw. erstellen Sie den Integrationsbenutzer. Notieren Sie sich den Inhalt der Felder **Benutzername** und **Quellentyp**. Beispiel: Benutzer mit Namen **integration@example.com** aus der Quelle **Active Directory - ad**.
- 4 Wählen Sie **Authentifizierungsquellen** aus.
- 5 Identifizieren Sie die Authentifizierungsquelle, die dem **Quellentyp** aus Schritt 3 entspricht. Notieren Sie sich den Inhalt des Felds **Quellanzeigename**. Beispiel: „ad“.
- 6 Der Benutzername, der auf der vRealize Log Insight-Benutzeroberfläche für die Verwaltung eingegeben werden sollte, setzt sich aus den Angaben in den Schritten 3 und 5 im Format „Benutzername@Quellenanzeigename“ zusammen. Beispiel: integration@example.com@ad.

Voraussetzungen

Vergewissern Sie sich, dass das Integrationsbenutzerkonto über Berechtigungen zur Manipulation von Objekten in vRealize Operations Manager verfügt. Weitere Informationen hierzu finden Sie unter [Erforderliche Mindestberechtigungen für ein lokales oder Active Directory-Benutzerkonto](#).

Erforderliche Mindestberechtigungen für ein lokales oder Active Directory-Benutzerkonto

Zur Integration von vRealize Log Insight in vRealize Operations Manager müssen Anmeldedaten für vRealize Log Insight zur Authentifizierung bei vRealize Operations Manager festgelegt werden. Zur Handhabung von Objekten in vRealize Operations Manager benötigt ein Benutzerkonto die erforderlichen Berechtigungen.

vRealize Operations Manager -Lizenz

Wenn Sie einem Benutzer Berechtigungen für den kontextbezogenen Start zuweisen, kann der Benutzer auch die Warnungsintegration konfigurieren. Verwenden Sie die Informationen in der Tabelle für die Warnungsintegration, um nur für die Warnungsintegration Berechtigungen zuzuweisen.

Tabelle 12-1. Warnungsintegration

Aktion	Auszuwählende Berechtigungen und Objekte
Erstellen Sie eine benutzerdefinierte Rolle mit den aufgeführten Berechtigungen.	<ol style="list-style-type: none"> 1 Administration -> Ressourcenartverwaltung [Alle überprüfen] 2 Administration -> Ressourcenverwaltung [Alle überprüfen] 3 Administration -> Rest-APIs <ol style="list-style-type: none"> a Alle anderen, Lese- und Schreib-APIs b Lesezugriff auf APIs
Weisen Sie die vorherige Rolle dem (neuen oder vorhandenen) lokalen oder Active Directory-Benutzer zu und wählen Sie zuzuweisende Objekte/Objekthierarchien aus.	<ol style="list-style-type: none"> 1 Adapterinstanz -> vRealizeOpsMgrAPI [Alle überprüfen] 2 vSphere-Hosts und -Cluster [Alle überprüfen] 3 vSphere-Netzwerk [Alle überprüfen] 4 vSphere-Speicher [Alle überprüfen]

Für die Durchführung eines kontextbezogenen Starts muss ein Benutzer über Administratorrechte verfügen. Wenn sowohl Warnungen als auch kontextbezogener Start aktiviert sind, ist ein Benutzer mit Administratorrechten erforderlich.

Aktion	Auszuwählende Berechtigungen und Objekte
Weisen Sie die Administratorrolle einem Benutzerkonto zu.	<p>Von der Registerkarte Objekte auf der Seite Gruppen und Berechtigungen zuweisen:</p> <ol style="list-style-type: none"> 1 Wählen Sie unter Rolle auswählen Administrator aus. 2 Wählen Sie Dem Benutzer diese Rolle zuweisen aus. 3 Wählen Sie Zugriff auf alle Objekte im System gewähren aus.

Konfigurieren von vRealize Log Insight zum Senden von Benachrichtigungsereignissen an vRealize Operations Manager

Sie können vRealize Log Insight konfigurieren, um Warnungsbenachrichtigungen an vRealize Operations Manager zu senden.

Sie können vRealize Log Insight in vRealize Operations Manager vApp und vRealize Operations Manager Installable integrieren. Die Integration in die Installable-Version erfordert zusätzliche Änderungen an der Konfiguration von vRealize Operations Manager. Informationen zur Konfiguration von vRealize Operations Manager Installable zur Integration in vRealize Log Insight finden Sie in der Anleitung *Erste Schritte für Log Insight*.

Bei der Integration von vRealize Log Insight-Warnungen mit vRealize Operations Manager können Sie alle Informationen über Ihre Umgebung in einer einzelnen Benutzeroberfläche anzeigen.

Sie können Benachrichtigungsereignisse von mehreren vRealize Log Insight-Instanzen aus an eine einzelne vRealize Operations Manager-Instanz senden. Sie können den kontextbezogenen Start für eine einzelne vRealize Log Insight-Instanz pro vRealize Operations Manager-Instanz aktivieren.


vRealize Log Insight verwendet die vRealize Operations Manager-REST-API für das Erstellen von Ressourcen und Beziehungen in vRealize Operations Manager zum Konfigurieren des Adapters für den kontextbezogenen Start.

Voraussetzungen

- Erstellen Sie ein Integrationsbenutzerkonto in vRealize Operations Manager mit den erforderlichen Berechtigungen. Weitere Informationen finden Sie unter [Anforderungen für die Integration in vRealize Operations Manager](#).
- Sie müssen die IP-Adresse oder den Hostnamen der Zielinstanz von vRealize Operations Manager kennen.
- 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.

Hinweis In einer Umgebung, in der ein vRealize Operations Manager-Cluster mit einem konfigurierten Lastausgleichsdienst ausgeführt wird, können Sie die IP-Adresse des Lastausgleichsdienstes verwenden, falls verfügbar.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Integration, select **vRealize Operations Manager**.
- 3 Geben Sie die IP-Adresse oder den Hostnamen des Master-Knotens oder des Lastausgleichsdienstes (falls konfiguriert) ein. Verwenden Sie vRealize Operations Manager-Anmeldedaten und klicken Sie auf **Verbindung testen**. vRealize Log Insight verwendet Anmeldedaten, um Benachrichtigungsereignisse an vRealize Operations Manager weiterzugeben. Vergewissern Sie sich, dass der konfigurierte Benutzer über die Mindestberechtigungen verfügt, die für eine funktionierende Integration erforderlich sind. Weitere Informationen hierzu finden Sie unter [Erforderliche Mindestberechtigungen für ein lokales oder Active Directory-Benutzerkonto](#).
- 4 Wählen Sie im Bereich „vRealize Operations Manager“ **Integration von Warnungen aktivieren** aus.
- 5 Click **Save**.

Weiter

- Die von vRealize Log Insight gesendeten Benachrichtigungsereignisse werden auf den betreffenden Seiten in der vRealize Operations Manager-Benutzeroberfläche angezeigt.

Aktivieren des kontextbezogenen Starts für vRealize Log Insight in vRealize Operations Manager

Sie können vRealize Operations Manager so konfigurieren, dass mit vRealize Log Insight in Zusammenhang stehende Menüelemente angezeigt werden und vRealize Log Insight mit einer objektspezifischen Abfrage gestartet wird.

Sie können vRealize Log Insight in vRealize Operations Manager vApp und vRealize Operations Manager Installable integrieren.

Die Integration in die vApp-Installation und in Installable (Windows, Linux) erfordert zusätzliche Änderungen der vRealize Operations Manager-Konfiguration. Weitere Informationen finden Sie im Thema zur Installation des vRealize Log Insight Management Pack (Adapter) in vRealize Operations Manager 6.x und höher im [vRealize Log Insight 4.0-Informationscenter](#).

Beachten Sie, dass das vRealize vRealize Log Insight Management Pack in vRealize Operations Manager 6.0 und höher vorinstalliert ist und dafür keine Konfigurationsänderungen erforderlich sind.


vRealize Operations Manager Installable (Windows-Version) wird ab vRealize Operations Manager 6.5 nicht mehr unterstützt.

Wichtig Eine Instanz von vRealize Operations Manager unterstützt den kontextbezogenen Start für nur eine Instanz von vRealize Log Insight. Da vRealize Log Insight nicht überprüft, ob bei vRealize Operations Manager bereits andere Instanzen registriert sind, könnten Sie die Einstellungen eines anderen Benutzers außer Kraft setzen.

Voraussetzungen

- 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.
- Sie müssen die IP-Adresse oder den Hostnamen der Zielinstanz von vRealize Operations Manager kennen.
- Stellen Sie sicher, dass Sie über die erforderlichen Benutzeranmeldedaten verfügen. Weitere Informationen hierzu finden Sie unter [Erforderliche Mindestberechtigungen für ein lokales oder Active Directory-Benutzerkonto](#).
- Wenn Sie vRealize Operations Manager 6.5 oder höher einsetzen, verwenden Sie die Vorgehensweise für die Aktivierung des kontextbezogenen Starts im [vRealize Operations Manager 6.5-Informationscenter](#).

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Integration, select **vRealize Operations Manager**.
- 3 Geben Sie die IP-Adresse oder den FQDN des vRealize Operations Manager-Master-Knotens oder des Lastausgleichsdiensts (falls konfiguriert) ein und klicken Sie auf **Verbindung testen**.

Hinweis Für den kontextbezogenen Start müssen Sie einen vRealize Operations Manager-Benutzer mit Administratorrechten angeben.

- 4 Click **Save**.

vRealize Log Insight konfiguriert die vRealize Operations Manager-Instanz. Dieser Vorgang kann einige Minuten dauern.

Es werden mit vRealize Log Insight in Zusammenhang stehende Elemente in den Menüs von vRealize Operations Manager angezeigt.

Weiter

Starten Sie eine vRealize Log Insight-Abfrage aus der vRealize Operations Manager-Instanz. Siehe [Kontextbezogener Start von vRealize Log Insight](#).

Kontextbezogener Start von vRealize Log Insight

Wenn Sie den kontextbezogenen Start für vRealize Log Insight aktivieren, wird eine vRealize Log Insight-Ressource in vRealize Operations Manager erstellt.

Der Ressourcenbezeichner enthält die IP-Adresse der vRealize Log Insight-Instanz und wird von vRealize Operations Manager zum Öffnen von vRealize Log Insight verwendet.

Kontextbezogener Start in vRealize Operations Manager 6.5 und höher

Informationen zur Aktivierung eines kontextbezogenen Starts finden Sie im [vRealize Operations Manager-Informationscenter](#).

Kontextbezogener Start in der vSphere-Benutzeroberfläche von vRealize Operations Manager 6.4 und früher

Die kontextbezogenen Startoptionen in Verbindung mit vRealize Log Insight werden im Dropdown-Menü **Aktionen** der vSphere-Benutzeroberfläche angezeigt. Sie können diese Menüelemente verwenden, um vRealize Log Insight zu öffnen und um Protokollereignisse von einem Objekt in vRealize Operations Manager zu suchen.

Welche kontextbezogene Startaktion verfügbar ist, hängt vom Objekt ab, das Sie im vRealize Operations Manager-Bestand auswählen. Der Zeitraum der Abfragen ist auf 60 Minuten vor dem Klicken auf eine kontextbezogene Startoption begrenzt.

Tabelle 12-3. Objekte in der vRealize Operations Manager -Benutzeroberfläche und deren entsprechende kontextbezogene Startoptionen und -aktionen

In vRealize Operations Manager ausgewählte Objekte	Kontextbezogene Startoption im Dropdown-Menü Aktionen	Aktion in vRealize Operations Manager	Aktion in vRealize Log Insight
World	Öffnen von vRealize Log Insight	Öffnet vRealize Log Insight.	vRealize Log Insight zeigt die Registerkarte Interaktive Analyse an.
vCenter Server	Öffnen von vRealize Log Insight	Öffnet vRealize Log Insight.	vRealize Log Insight zeigt die Registerkarte Interaktive Analyse an.

Tabelle 12-3. Objekte in der vRealize Operations Manager -Benutzeroberfläche und deren entsprechende kontextbezogene Startoptionen und -aktionen (Fortsetzung)

In vRealize Operations Manager ausgewählte Objekte	Kontextbezogene Startoption im Dropdown-Menü Aktionen	Aktion in vRealize Operations Manager	Aktion in vRealize Log Insight
Datencenter	Suchen nach Protokollen in vRealize Log Insight	Öffnet vRealize Log Insight und übergibt die Ressourcennamen aller Hostsysteme unter dem ausgewählten Datencenterobjekt.	vRealize Log Insight zeigt die Registerkarte Interaktive Analyse an und führt eine Abfrage durch, um Protokollereignisse zu finden, die Hostnamen des Datencenters enthalten.
Cluster	Suchen nach Protokollen in vRealize Log Insight	Öffnet vRealize Log Insight und übergibt die Ressourcennamen aller Hostsysteme unter dem ausgewählten Clusterobjekt.	vRealize Log Insight zeigt die Registerkarte Interaktive Analyse an und führt eine Abfrage durch, um Protokollereignisse zu finden, die Hostnamen des Clusters enthalten.
Hostsystem	Suchen nach Protokollen in vRealize Log Insight	Öffnet vRealize Log Insight und übergibt den Ressourcennamen des ausgewählten Hostobjekts.	vRealize Log Insight zeigt die Registerkarte Interaktive Analyse an und führt eine Abfrage durch, um Protokollereignisse zu finden, die den Namen des ausgewählten Hostsystems enthalten.
Virtuelle Maschine	Suchen nach Protokollen in vRealize Log Insight	Öffnet vRealize Log Insight und übergibt die IP-Adresse der ausgewählten virtuellen Maschine und den Ressourcennamen des verbundenen Hostsystems.	vRealize Log Insight zeigt die Registerkarte Interaktive Analyse an und führt eine Abfrage durch, um Protokollereignisse zu finden, die die IP-Adresse der virtuellen Maschine und den Namen des Hosts, auf dem sich die virtuelle Maschine befindet, enthalten.

Wenn Sie auf der Registerkarte **Warnungen** eine Warnung auswählen und dann im Kontextmenü auf **Protokolle in Log Insight suchen** klicken, wird der Zeitraum auf eine Stunde vor dem Auslösen der Warnung begrenzt. Wenn beispielsweise eine Warnung um 14:00 Uhr ausgelöst wurde, zeigt die Abfrage in vRealize Log Insight alle Protokollmeldungen an, die sich zwischen 13:00 und 14:00 Uhr ereigneten. Dies hilft Ihnen, Ereignisse zu identifizieren, die die Warnung ausgelöst haben könnten.

Sie können vRealize Log Insight über Metrikdiagramme in vRealize Operations Manager öffnen. Der Zeitraum der Abfrage, die von vRealize Log Insight ausgeführt wird, entspricht dem Zeitraum des Metrikdiagramms.

Hinweis Die Zeiten, die in vRealize Log Insight und den Metrikdiagrammen in vRealize Operations Manager angezeigt werden, können unterschiedlich sein, wenn die Zeiteinstellung der virtuellen Appliances unterschiedlich ist.

Kontextbezogener Start in der Benutzeroberfläche von vRealize Operations Manager 6.4 und früher



Das Symbol für den kontextbezogenen Start wird zwar auf mehreren Seiten der Benutzeroberfläche angezeigt, Sie können jedoch vRealize Log Insight nur von den Seiten aus starten, auf denen die vRealize Log Insight-Benachrichtigungsereignisse angezeigt werden:

- Seite „Warnungen – Überblick“.
- Seite „Warnung – Zusammenfassung“ einer vRealize Log Insight-Benachrichtigungswarnung.
- Widgets „Warnungen“ auf Ihren Dashboards, wenn eine vRealize Log Insight-Benachrichtigungswarnung ausgewählt ist.

Wenn Sie in der benutzerdefinierten Benutzeroberfläche ein vRealize Log Insight-Benachrichtigungsereignis auswählen, können Sie unter zwei kontextbezogenen Startaktionen wählen.

Tabelle 12-4. Kontextbezogene Startoptionen und -aktionen in der Benutzeroberfläche von vRealize Operations Manager

Kontextbezogene Startoption in vRealize Operations Manager	Aktion in vRealize Operations Manager	Aktion in vRealize Log Insight
Öffnen von vRealize Log Insight	Öffnet vRealize Log Insight.	vRealize Log Insight zeigt die Registerkarte Dashboards an und lädt das Dashboard „vSphere-Übersicht“.
Suchen nach Protokollen in vRealize Log Insight	Öffnet vRealize Log Insight und übergibt den Bezeichner der Abfrage, die das Benachrichtigungsereignis ausgelöst hat.	vRealize Log Insight zeigt die Registerkarte Interaktive Analyse an und führt die Abfrage durch, die das Benachrichtigungsereignis ausgelöst hat.

Wenn Sie eine Warnung auswählen, die nicht von vRealize Log Insight stammt, enthält das kontextbezogene Startmenü das Menüelement **VM- und Hostprotokolle in vRealize Log Insight suchen**. Wenn Sie dieses Menüelement wählen, öffnet vRealize Operations Manager vRealize Log Insight und übergibt die Bezeichner des Objekts, das die Warnung ausgelöst hat. vRealize Log Insight verwendet die Ressourcenbezeichner, um eine Suche in den verfügbaren Protokollereignissen durchzuführen.

Kontextbezogener Start in beide Richtungen

Der kontextbezogene Start ist auch von vRealize Log Insight bis vRealize Operations Manager verfügbar.

Wenn Sie vRealize Log Insight in vRealize Operations Manager integrieren, können Sie einen kontextbezogenen Start von einem vRealize Log Insight-Ereignis ausführen, indem Sie das Zahnradsymbol links vom Ereignis auswählen und die Option zur Anzeige in vRealize Operations Manager auswählen.

Weitere Informationen zum kontextbezogenen Start von vRealize Operations Manager in vRealize Log Insight finden Sie unter [Kontextbezogener Start von vRealize Log Insight](#).

Vorgehensweise

- 1 Rufen Sie in vRealize Log Insight die Registerkarte **Interaktive Analyse** auf.
- 2 Suchen Sie ein Ereignis, das Felder zur Bestandslistenzuordnung enthält, und halten Sie den Mauszeiger über das Ereignis.
- 3 Klicken Sie auf das Zahnradsymbol und wählen Sie **Offene Analyse** in vRealize Operations Manager aus dem Dropdown-Menü aus.

Ein neues Browserfenster wird geöffnet, in dem Sie zur vRealize Operations Manager-Instanz geleitet werden, die in vRealize Log Insight integriert ist. Nach der Authentifizierung werden Sie zum Abschnitt **Umgebung > Analyse** von vRealize Operations Manager mit dem ausgewählten Objekt geleitet.

Hinweis Wenn mehrere vRealize Log Insight-Instanzen mit der gleichen vRealize Operations Manager-Instanz verbunden sind, verfügt nur die letzte vRealize Log Insight-Instanz, die mit vRealize Operations Manager integriert wurde, über die Funktion des kontextbezogenen Starts. Das bedeutet auch, dass die Funktion des kontextbezogenen Starts jedes Mal überschrieben wird, wenn eine vRealize Log Insight-Instanz in eine vRealize Operations Manager-Instanz integriert wird, die zuvor in eine andere vRealize Log Insight-Instanz integriert war.

Deaktivieren des kontextbezogenen Starts für vRealize Log Insight in vRealize Operations Manager

Sie können den vRealize Log Insight-Adapter von der vRealize Operations Manager-Instanz deinstallieren, um mit vRealize Log Insight verbundene Menüelemente von der Benutzeroberfläche von vRealize Operations Manager zu entfernen.


Über die Benutzeroberfläche von vRealize Log Insight für Administratoren können Sie den kontextbezogenen Start deaktivieren. Wenn Sie nicht auf vRealize Log Insight zugreifen können oder die vRealize Log Insight-Instanz gelöscht wird, bevor die Verbindung mit vRealize Operations Manager deaktiviert wird, können Sie die Registrierung von vRealize Log Insight über die Administrations-Benutzeroberfläche von vRealize Operations Manager aufheben. Weitere diesbezügliche Informationen finden Sie in der Hilfe des Verwaltungsportals von vRealize Operations Manager.

Vorsicht Eine Instanz von vRealize Operations Manager unterstützt den kontextbezogenen Start für nur eine Instanz von vRealize Log Insight. Wenn eine andere vRealize Log Insight-Instanz registriert wurde, nachdem Sie die Instanz, die Sie deaktivieren möchten, registriert haben, setzt die zweite Instanz die Einstellungen der ersten außer Kraft, ohne Sie zu benachrichtigen.

Voraussetzungen

- 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.

Vorgehensweise

- 1 Click the configuration drop-down menu icon  and select **Administration**.
- 2 Under Integration, select **vRealize Operations Manager**.
- 3 Deaktivieren Sie das Kontrollkästchen **Kontextbezogenen Start aktivieren**.
- 4 Click **Save**.

vRealize Log Insight konfiguriert die vRealize Operations Manager-Instanz so, dass diese den vRealize Log Insight-Adapter entfernt. Dieser Vorgang kann einige Minuten dauern.

Hinzufügen von DNS-Suchpfad und -domäne

Sie können einen DNS-Suchpfad und eine DNS-Suchdomäne hinzufügen, um den vRealize Operations Manager-Inventarabgleich zu optimieren.

Durch das Hinzufügen eines DNS-Suchpfads und einer DNS-Suchdomäne wird der Abgleich verbessert, wenn die Beschriftungs- und Suchdomäne einer virtuellen Maschine in Bezug auf die IP-Adresse des Hosts aufgelöst wird, welcher Protokollmeldungen an vRealize Log Insight sendet. Beispiel: Wenn Sie über eine virtuelle Maschine mit der Bezeichnung „linux_01“ in vRealize Operations Manager verfügen und wenn der Hostname „linux_01.company.com“ in 192.168.10.10 aufgelöst wird, kann vRealize Log Insight durch das Hinzufügen einer Suchdomäne diese Ressource erkennen und abgleichen.

Vorgehensweise

- 1 Führen Sie ein Herunterfahren des Gasts der virtuellen vRealize Log Insight-Appliance aus.
- 2 Nach dem Herunterfahren der virtuellen Maschine wählen Sie **Einstellungen bearbeiten** aus.
- 3 Klicken Sie auf die Registerkarte **Optionen**.
- 4 Klicken Sie unter **vApp-Optionen** > **Erweitert** auf **Eigenschaften**.
- 5 Suchen Sie die Schlüssel `vami.searchpath.VMware_vCenter_Log_Insight` und `vami.domain.VMware_vCenter_Log_Insight`.
Falls die Schlüssel nicht vorhanden sind, erstellen Sie sie.
- 6 Legen Sie den DNS-Suchpfad und die DNS-Suchdomäne fest.
- 7 Schalten Sie die virtuelle Appliance ein.

Weiter

Nach dem Starten von vRealize Log Insight können Sie die DNS-Konfiguration validieren, indem Sie sich anmelden und den Inhalt der Datei `/etc/resolv.conf` anzeigen. Gegen Ende der Datei finden Sie die Such- und Domänenoptionen.

Entfernen des vRealize Log Insight -Adapters

Wenn Sie den kontextbezogenen Start für eine Instanz von vRealize Operations Manager 6.2 und höher aktivieren, erstellt vRealize Log Insight eine Instanz des vRealize Log Insight-Adapters in der vRealize Operations Manager-Instanz.

Die Instanz des Adapters bleibt in der vRealize Operations Manager-Instanz, wenn Sie vRealize Log Insight deinstallieren. Dadurch werden die Elemente des Menüs für den kontextbezogenen Start weiterhin im Menü „Aktionen“ angezeigt und verweisen auf eine vRealize Log Insight-Instanz, die nicht mehr existiert.

Um den kontextbezogenen Start in vRealize Operations Manager zu deaktivieren, müssen Sie den vRealize Log Insight-Adapter aus der vRealize Operations Manager-Instanz entfernen.

Sie können das Befehlszeilendienstprogramm cURL verwenden, um REST-Anrufe an vRealize Operations Manager zu senden.

Hinweis Diese Schritte sind nur erforderlich, wenn der kontextbezogene Start aktiviert wurde.

Voraussetzungen

- Überprüfen Sie, ob cURL auf Ihrem System installiert ist. Beachten Sie, dass das Tool in der vRealize Operations Manager virtuellen Appliance vorinstalliert ist und die Schritte von der Appliance aus über die IP-Adresse 127.0.0.1 vorgenommen werden können.
- Sie müssen die IP-Adresse oder den Hostnamen der Zielinstanz von vRealize Operations Manager kennen.
- Abhängig von Ihrer vRealize Operations Manager-Lizenz müssen Sie überprüfen, ob Sie über die minimalen Benutzeranmeldedaten verfügen, die zum Entfernen des Management Pack erforderlich sind. Weitere Informationen hierzu finden Sie unter [Erforderliche Mindestberechtigungen für ein lokales oder Active Directory-Benutzerkonto](#).

Vorgehensweise

- 1 Führen Sie in cURL die folgende Abfrage für die virtuelle vRealize Operations Manager-Appliance aus, um den vRealize Log Insight-Adapter zu finden.

```
curl -k -u "admin" https://ipaddress/suite-  
api/api/adapterkinds/LogInsight/resourcekinds/LogInsightLogServer/resources
```

Admin als Anmeldename des Administrators und *IP-Adresse* als IP-Adresse (oder Hostname) der vRealize Operations Manager-Instanz. Sie werden dazu aufgefordert, das Kennwort für folgenden Benutzer einzugeben: *Admin*.

Ermitteln Sie in der cURL-Ausgabe den GUID-Wert für den Bezeichner: <ops:resource creationTime="{TIMESTAMP}" identifier="{GUID}">. Sie können diesen GUID-Wert im nachfolgenden Befehl zum Entfernen der Adapterinstanz verwenden.

- 2 Führen Sie den folgenden Befehl aus, um den vRealize Log Insight-Adapter zu entfernen:

```
curl -k -u "admin" -X DELETE https://ipaddress/suite-api/api/adapters/{GUID}
```

Admin als Anmeldename des Administrators und *IP-Adresse* als IP-Adresse (oder Hostname) der vRealize Operations Manager-Instanz. Sie werden dazu aufgefordert, das Kennwort für folgenden Benutzer einzugeben: *Admin*.

Elemente des kontextbezogenen Starts von vRealize Log Insight werden aus den Menüs in vRealize Operations Manager entfernt. Weitere Informationen zum kontextbezogenen Start finden Sie unter *Kontextbezogener Start von vRealize Log Insight* in der produktbezogenen Hilfe von vRealize Log Insight.

vRealize Operations Manager -Inhaltspaket für vRealize Log Insight

Das vRealize Operations Manager-Inhaltspaket für vRealize Log Insight enthält Dashboards, extrahierte Felder, gespeicherte Abfragen und Warnungen, die zur Analyse aller von einer vRealize Operations Manager-Instanz umgeleiteten Protokolle verwendet werden.

Das vRealize Operations Manager-Inhaltspaket bietet die Möglichkeit, alle von einer vRealize Operations Manager-Instanz umgeleiteten Protokolle zu analysieren. Das Inhaltspaket enthält Dashboards, Abfragen und Warnungen, die dem vRealize Operations Manager-Administrator die Diagnose und Fehlerbehebung ermöglichen sollen. Die Dashboards sind zur besseren Verwaltbarkeit nach den Hauptkomponenten von vRealize Operations Manager wie Analyse, Benutzeroberfläche und Adapter gruppiert. Sie können verschiedene Alarme für das Versenden von Benachrichtigungseignissen in vRealize Operations Manager und von E-Mails an Administratoren aktivieren.

Das Inhaltspaket von vRealize Operations Manager kann über https://solutionexchange.vmware.com/store/loginsight?src=Product_Product_LogInsight_YES_US heruntergeladen werden.

Siehe [Arbeiten mit Inhaltspaketen](#).

Sicherheitsüberlegungen für vRealize Log Insight

13

Nutzen Sie die vRealize Log Insight-Funktionen, um Ihre Umgebung vor Angriffen zu schützen.

Dieses Kapitel behandelt die folgenden Themen:

- [Ports und externe Schnittstellen](#)
- [vRealize Log Insight-Konfigurationsdateien](#)
- [Öffentlicher Schlüssel, Zertifikat und Keystore für vRealize Log Insight](#)
- [vRealize Log Insight-Lizenz und EULA-Datei](#)
- [vRealize Log Insight-Protokolldateien](#)
- [vRealize Log InsightBenutzerkonten](#)
- [vRealize Log Insight-Firewall-Empfehlungen](#)
- [Sicherheits-Updates und Patches](#)

Ports und externe Schnittstellen

vRealize Log Insight verwendet bestimmte erforderliche Dienste, Ports und externe Schnittstellen.

Kommunikationsports

vRealize Log Insight verwendet die Kommunikationsports und -protokolle, die in diesem Thema aufgeführt sind. Die erforderlichen Ports sind danach sortiert, ob sie für Quellen, für die Benutzeroberfläche, zwischen Clustern oder für externe Dienste erforderlich sind oder ob sie von einer Firewall auf sichere Weise blockiert werden können. Manche Ports werden nur verwendet, wenn Sie die entsprechende Integration aktivieren.

Hinweis vRealize Log Insight unterstützt das WAN-Clustering nicht (dies wird auch als Geo-Clustering, Hochverfügbarkeits-Clustering oder Remote-Clustering bezeichnet). Alle Knoten im Cluster müssen in demselben Layer 2-LAN bereitgestellt werden. Darüber hinaus müssen die in diesem Abschnitt beschriebenen Ports zwischen den Knoten geöffnet sein, um eine ordnungsgemäße Kommunikation zu gewährleisten.

Der Netzwerkdatenverkehr von vRealize Log Insight stammt aus verschiedenen Quellen.

Admin-Workstation	Die Maschine, die von einem Systemadministrator zur Fernverwaltung der virtuellen vRealize Log Insight-Appliance verwendet wird.
Benutzer-Workstation	Die Maschine, auf der ein Benutzer von vRealize Log Insight einen Browser für den Zugriff auf die Web-Oberfläche von vRealize Log Insight verwendet.
Protokolle sendendes System	Der Endpoint, der zu Analyse- und Suchzwecken Protokolle an vRealize Log Insight sendet. Solche Endpoints können z. B. ESXi-Hosts, virtuelle Maschinen oder jedes System mit einer IP-Adresse sein.
Log Insight Agents	Der Agent, der sich auf einer Windows- oder Linux-Maschine befindet und Ereignisse und Protokolle des Betriebssystems über APIs an vRealize Log Insight sendet.
vRealize Log Insight-Appliance	Jede beliebige virtuelle vRealize Log Insight-Appliance (Master oder Worker), auf der sich die vRealize Log Insight-Dienste befinden. Das Basisbetriebssystem der Appliance ist SUSE 11 SP3.

Erforderliche Ports für Daten sendende Quellen

Die folgenden Ports müssen geöffnet sein, um Netzwerkdatenverkehr aus Quellen, die Daten an vRealize Log Insight senden, zu ermöglichen, sowohl für Verbindungen von außerhalb des Clusters als auch für Verbindungen zum Lastenausgleich zwischen Clusterknoten.

Quelle	Ziel	Port	Protokoll	Dienstbeschreibung
Protokolle sendendes System	vRealize Log Insight-Appliance	514	TCP, UDP	Als Weiterleitungsziel konfigurierter ausgehender Syslog-Datenverkehr
Protokolle sendendes System	vRealize Log Insight-Appliance	1514, 6514	TCP	Syslog-Daten über SSL
vRealize Log Insight-Agenten	vRealize Log Insight-Appliance	9000	TCP	Log Insight Ingestion-API
vRealize Log Insight-Agenten	vRealize Log Insight-Appliance	9543	TCP	Ingestion-API von Log Insight über SSL

Erforderliche Ports für die Benutzeroberfläche

Die folgenden Ports müssen geöffnet sein, um Netzwerkdatenverkehr über die vRealize Log Insight-Benutzeroberfläche zu ermöglichen, sowohl für Verbindungen außerhalb des Clusters als auch für Verbindungen zum Lastenausgleich zwischen Clusterknoten.

Quelle	Ziel	Port	Protokoll	Dienstbeschreibung
Admin-Workstation	vRealize Log Insight-Appliance	22	TCP	SSH: Secure Shell-Konnektivität
Benutzer-Workstation	vRealize Log Insight-Appliance	80	TCP	HTTP: Web-Oberfläche
Benutzer-Workstation	vRealize Log Insight-Appliance	443	TCP	HTTPS: Web-Oberfläche

Erforderliche Ports zwischen Clusterknoten

Um maximale Sicherheit zu gewährleisten, sollten die folgenden Ports ausschließlich an einem vRealize Log Insight-Master-Knoten für den Netzwerkzugriff von Worker-Knoten aus geöffnet sein. Diese Ports werden zusätzlich zu den Ports zum Lastenausgleich zwischen Clusterknoten für Quellen und den Datenverkehr über die Benutzeroberfläche geöffnet.

Quelle	Ziel	Port	Protokoll	Dienstbeschreibung
vRealize Log Insight-Appliance	vRealize Log Insight-Appliance	7000	TCP	Cassandra-Replizierung und -Abfrage
vRealize Log Insight-Appliance	vRealize Log Insight-Appliance	9042	TCP	Cassandra-Dienst für native Protokoll-Clients
vRealize Log Insight-Appliance	vRealize Log Insight-Appliance	9160	TCP	Cassandra-Dienst für Thrift-Clients
vRealize Log Insight-Appliance	vRealize Log Insight-Appliance	59778, 16520-16580	TCP	Thrift-Dienst von vRealize Log Insight

Erforderliche Ports für externe Dienste

Die folgenden Ports müssen für ausgehenden Netzwerkdatenverkehr von vRealize Log Insight-Clusterknoten zu Remotediensten geöffnet sein.

Quelle	Ziel	Port	Protokoll	Dienstbeschreibung
vRealize Log Insight-Appliance	NTP-Server	123	UDP	NTPD: sorgt für die NTP-Uhrzeitsynchronisierung Hinweis Der Port ist nur dann geöffnet, wenn Sie die NTP-Uhrzeitsynchronisierung verwenden.
vRealize Log Insight-Appliance	Mail-Server	25	TCP	SMTP: Mail-Dienst für ausgehende Warnungen
vRealize Log Insight-Appliance	Mail-Server	465	TCP	SMTPS: Mail-Dienst über SSL für ausgehende Warnungen

Quelle	Ziel	Port	Protokoll	Dienstbeschreibung
vRealize Log Insight-Appliance	DNS Server	53	TCP, UDP	DNS: Namensauflösungsdienst
vRealize Log Insight-Appliance	AD-Server	389	TCP, UDP	Active Directory
vRealize Log Insight-Appliance	AD-Server	636	TCP	Active Directory über SSL
vRealize Log Insight-Appliance	AD-Server	3268	TCP	Globaler Active Directory-Katalog
vRealize Log Insight-Appliance	AD-Server	3269	TCP	SSL für globalen Active Directory-Katalog
vRealize Log Insight-Appliance	AD-Server	88	TCP, UDP	Kerberos
vRealize Log Insight-Appliance	vCenter Server	443	TCP	vCenter Server-Webservice
vRealize Log Insight-Appliance	vRealize Operations Manager-Appliance	443	TCP	vRealize Operations-Webservice
vRealize Log Insight-Appliance	Protokollmanager eines Drittanbieters	514	TCP, UDP	Syslog-Daten
vRealize Log Insight-Appliance	Protokollmanager eines Drittanbieters	9000	CFAPI	Als Weiterleitungsziel konfigurierter ausgehender Log Insight-Erfassungs-API(CFAPI)-Datenverkehr
vRealize Log Insight-Appliance	Protokollmanager eines Drittanbieters	9543	CFAPI	Als Weiterleitungsziel mit Verschlüsselung (SSL/TLS) konfigurierter ausgehender Log Insight-Erfassungs-API(CFAPI)-Datenverkehr

Ports, die blockiert werden können

Die folgenden Ports sind offen, werden von vRealize Log Insight aber nicht verwendet. Diese Ports können auf sichere Weise von einer Firewall blockiert werden.

Ziel	Port	Protokoll	Dienstbeschreibung
vRealize Log Insight-Appliance	111	TCP, UDP	RPCbind-Dienst, der RPC-Programmnummern in universelle Adressen konvertiert
Tomcat-Dienst der vRealize Log Insight-Appliance	9007	TCP	Tomcat-Dienste

vRealize Log Insight -Konfigurationsdateien

Einige Konfigurationsdateien enthalten Einstellungen, die sich auf die Sicherheit von vRealize Log Insight auswirken.

Hinweis Auf sämtliche sicherheitsbezogenen Ressourcen kann über das Root-Konto zugegriffen werden. Der Schutz dieses Kontos ist für die Sicherheit von vRealize Log Insight unabdingbar.

Tabelle 13-1. Log Insight-Konfigurationsdateien

Datei	Beschreibung
/usr/lib/loginsight/application/etc/loginsight-config-base.xml	Die standardmäßige Systemkonfiguration für vRealize Log Insight.
/storage/core/loginsight/config/loginsight-config.xml#number	Die (von der standardmäßigen Systemkonfiguration) abgeänderte Systemkonfiguration für vRealize Log Insight.
/usr/lib/loginsight/application/etc/jaas.conf	Die Konfiguration für die Active Directory-Integration.
/usr/lib/loginsight/application/etc/3rd_config/server.xml	Die Systemkonfiguration für Apache Tomcat-Server.
/storage/var/loginsight/apache-tomcat/conf/tomcat-users.xml	Die Systemkonfiguration für Apache Tomcat-Server.
/usr/lib/loginsight/application/3rd_party/apache-tomcat-*/conf/server.xml	Die Systemkonfiguration für Apache Tomcat-Server.
/usr/lib/loginsight/application/3rd_party/apache-tomcat-*/conf/tomcat-users.xml	Benutzerinformationen für Apache Tomcat-Server.

Öffentlicher Schlüssel, Zertifikat und Keystore für vRealize Log Insight

Der öffentliche Schlüssel, das Zertifikat und der Keystore von vRealize Log Insight befinden sich auf der virtuellen vRealize Log Insight-Appliance.

Hinweis Auf sämtliche sicherheitsbezogenen Ressourcen kann über das Root-Konto zugegriffen werden. Der Schutz dieses Kontos ist für die Sicherheit von vRealize Log Insight unabdingbar.

- /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

vRealize Log Insight -Lizenz und EULA-Datei

Die Endbenutzer-Lizenzvereinbarung (End-User License Agreement, EULA) und die Lizenzdatei befinden sich auf der virtuellen vRealize Log Insight-Appliance.

Hinweis Auf sämtliche sicherheitsbezogenen Ressourcen kann über das Root-Konto zugegriffen werden. Der Schutz dieses Kontos ist für die Sicherheit von vRealize Log Insight unabdingbar.

Datei	Speicherort
Lizenz	/usr/lib/loginsight/application/etc/license/loginsight_dev.dlf
Lizenz	/usr/lib/loginsight/application/etc/license/loginsight_cpu.dlf
Lizenz	/usr/lib/loginsight/application/etc/license/loginsight_osi.dlf
Lizenzschlüsseldatei	/usr/lib/loginsight/application/etc/license/loginsight_license.bak
Endbenutzer-Lizenzvereinbarung	/usr/lib/loginsight/application/etc/license/release/eula.txt

vRealize Log Insight -Protokolldateien

Die Dateien, die Systemmeldungen enthalten, befinden sich auf der virtuellen vRealize Log Insight-Appliance.

Datei	Beschreibung
/storage/var/loginsight/alert.log	Dient zur Verfolgung von Informationen zu benutzerdefinierten Warnungen, die ausgelöst wurden.
/storage/var/loginsight/apache-tomcat/logs/*.log	Dient zur Verfolgung von Ereignissen auf dem Apache Tomcat-Server.
/storage/var/loginsight/cassandra.log	Dient zur Verfolgung der Speicherung von Cluster-Konfigurationen und von deren Replikation in Apache Cassandra.
/storage/var/loginsight/plugins/vsphere/li-vsphere.log	Dient zur Verfolgung von Ereignissen in Verbindung mit der Integration in vSphere Web Client.
/storage/var/loginsight/loginsight_daemon_stdout.log	Wird für die Standardausgabe des vRealize Log Insight-Daemons verwendet.
/storage/var/loginsight/phonehome.log	Dient zur Verfolgung von Informationen zur Trace-Datenerfassung, die an VMware gesendet wird (sofern aktiviert).
/storage/var/loginsight/pi.log	Dient zur Verfolgung von Start- und Stopp-Ereignissen in der Datenbank.
/storage/var/loginsight/runtime.log	Dient zur Verfolgung aller Laufzeitinformationen in Verbindung mit vRealize Log Insight.
/var/log/firstboot/stratavm.log	Dient zur Verfolgung der Ereignisse, die beim erstmaligen Starten und Konfigurieren der virtuellen vRealize Log Insight-Appliance auftreten.

Datei	Beschreibung
/storage/var/loginsight/systemalert.log	Dient zur Verfolgung von Informationen zu von vRealize Log Insight gesendeten Systembenachrichtigungen. Jede Warnung wird als ein JSON-Eintrag aufgeführt.
/storage/var/loginsight/systemalert_worker.log	Dient zur Verfolgung von Informationen zu Systembenachrichtigungen, die von einem vRealize Log Insight-Worker-Knoten gesendet werden. Jede Warnung wird als ein JSON-Eintrag aufgeführt.
/storage/var/loginsight/ui.log	Dient zur Verfolgung von Ereignissen in Verbindung mit der Benutzeroberfläche von vRealize Log Insight.
/storage/var/loginsight/ui_runtime.log	Dient zur Verfolgung von Laufzeit-Ereignissen in Verbindung mit der Benutzeroberfläche von vRealize Log Insight.
/storage/var/loginsight/upgrade.log	Dient zur Verfolgung von Ereignissen, die während eines vRealize Log Insight-Upgrades auftreten.
/storage/var/loginsight/usage.log	Dient zur Verfolgung aller Abfragen.
/storage/var/loginsight/vcenter_operations.log	Dient zur Verfolgung von Ereignissen in Verbindung mit der Integration von vRealize Operations Manager.
/storage/var/loginsight/watchdog_log*	Dient zur Verfolgung der Laufzeitergebnisse des Watchdog-Prozesses, der für den Neustart von vRealize Log Insight im Fall eines Herunterfahrens verantwortlich ist.

Sicherheitsbezogene Protokollmeldungen

Die Datei `ui_runtime.log` enthält Protokollmeldungen zu Benutzer-Audits im folgenden Format:

- [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 out: 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)]]

vRealize Log Insight Benutzerkonten

Für die Verwaltung von vRealize Log Insight müssen ein System- und ein Root-Konto eingerichtet werden.

vRealize Log Insight -Root-Benutzer

Für vRealize Log Insight wird zurzeit das Root-Benutzerkonto als der Dienstbenutzer verwendet. Es wird kein weiterer Benutzer erstellt.

Sofern Sie die Root-Kennworteigenschaft nicht während der Bereitstellung festlegen, ist das Standard-Root-Kennwort leer. Sie müssen das Root-Kennwort während der erstmaligen Anmeldung bei der vRealize Log Insight-Konsole ändern.

SSH ist deaktiviert, bis das Standard-Root-Kennwort festgelegt wird.

Das Root-Kennwort muss die folgenden Anforderungen erfüllen:

- Es muss mindestens acht Zeichen enthalten.
- Es muss mindestens einen Großbuchstaben, einen Kleinbuchstaben, eine Ziffer und ein Sonderzeichen enthalten.

- Es darf nicht vier Mal dasselbe Zeichen enthalten.

vRealize Log Insight -Admin-Benutzer

Beim erstmaligen Start der virtuellen vRealize Log Insight-Appliance erstellt vRealize Log Insight das Admin-Benutzerkonto für die Web-Benutzeroberfläche.

Das Standard-Admin-Kennwort ist leer. Sie müssen das Admin-Kennwort während der Erstkonfiguration von vRealize Log Insight auf der Web-Benutzeroberfläche ändern.

Unterstützung für Active Directory

vRealize Log Insight unterstützt die Integration von Active Directory. Wenn vRealize Log Insight konfiguriert wurde, kann ein Benutzer anhand von Active Directory authentifiziert bzw. autorisiert werden.

Siehe [Aktivieren der Benutzerauthentifizierung durch Active Directory](#).

Standardbenutzern zugewiesene Berechtigungen

Der vRealize Log Insight-Dienstbenutzer verfügt über Root-Berechtigungen.

Der Admin-Benutzer der Web-Benutzeroberfläche verfügt lediglich für die vRealize Log Insight-Web-Benutzeroberfläche über Administratorrechte.

vRealize Log Insight -Firewall-Empfehlungen

Um von vRealize Log Insight erfasste vertrauliche Informationen zu schützen, platzieren Sie den oder die Server in einem Verwaltungsnetzwerksegment, das durch eine Firewall vom Rest des internen Netzwerks getrennt ist.

Erforderliche Ports

Die folgenden Ports müssen für Netzwerkdatenverkehr aus Quellen geöffnet sein, die Daten an vRealize Log Insight senden.

Port	Protokoll
514/UDP, 514/TCP	Syslog
1514/TCP, 6514/TCP	Syslog-TLS (SSL)
9000/TCP	vRealize Log Insight Ingestion-API
9543/TCP	vRealize Log Insight-Ingestion-API – TLS (SSL)

Die folgenden Ports müssen für Netzwerkdatenverkehr geöffnet sein, für den die vRealize Log Insight-Benutzeroberfläche verwendet wird.

Port	Protokoll
80/TCP	HTTP
443/TCP	HTTPS

Um die maximale Sicherheit zu gewährleisten, sollten die folgenden Portsätze ausschließlich an einem vRealize Log Insight-Master-Knoten für den Netzwerkzugriff von Worker-Knoten aus geöffnet sein.

Port	Protokoll
16520:16580/TCP	Thrift RPC
59778/TCP	log4j server
12543/TCP	Datenbankserver

Sicherheits-Updates und Patches

Die virtuelle vRealize Log Insight-Appliance verwendet SUSE Linux Enterprise Server 11 (x86_64), Version 11, Patch-Level 3 als Gastbetriebssystem.

VMware veröffentlicht Patches zur Behebung von Sicherheitsproblemen.

Beachten Sie vor der Anwendung eines Upgrades oder Patches auf das Gastbetriebssystem die Abhängigkeiten. Weitere Informationen hierzu finden Sie unter [Kapitel 6 Ports und externe Schnittstellen](#).

Sichern, Wiederherstellen und die Notfallwiederherstellung

14

Um kostspielige Ausfälle im Datacenter zu vermeiden, befolgen Sie diese Best Practices für die Durchführung einer Sicherung, Wiederherstellung und Notfallwiederherstellung von vRealize Log Insight.

Dieses Kapitel behandelt die folgenden Themen:

- [Sicherung, Wiederherstellung und Notfallwiederherstellung – Überblick](#)
- [Verwenden von statischen IP-Adressen und FQDN](#)
- [Planung und Vorbereitung](#)
- [Sichern von Knoten und Clustern](#)
- [Sichern von Linux- bzw. Windows-Agents](#)
- [Wiederherstellen von Knoten und Clustern](#)
- [Ändern von Konfigurationen nach der Wiederherstellung](#)
- [Überprüfen der Wiederherstellungen](#)
- [Notfallwiederherstellung](#)

Sicherung, Wiederherstellung und Notfallwiederherstellung – Überblick

VMware bietet ein umfassendes, integriertes Portfolio von Lösungen für Business Continuity und Disaster Recovery (BCDR), die hohe Verfügbarkeit, Datenschutz und Notfallwiederherstellung bieten.

Verwenden Sie die Informationen zu Sicherung, Wiederherstellung und Notfallwiederherstellung in diesem Dokument zu den vRealize Log Insight-Komponenten einschließlich Master-Knoten, Worker-Knoten und Ereignisweiterleitung.

- Informationen zu Master- und Worker-Cluster-Mitgliedern einschließlich Konfiguration, Protokolldaten und Anpassung finden Sie unter [Sichern von Knoten und Clustern](#).
- Informationen zur lokalen Konfiguration von Linux- oder Windows-Agents finden Sie unter [Sichern von Linux- bzw. Windows-Agents](#).

Die Informationen in diesem Dokument gelten nicht für die folgenden Tools und Produkte. Sie müssen die Informationen zu diesen Tools und Produkten aus verschiedenen Quellen abrufen.

- Drittanbieter-Tools, die speziell für die Sicherung, Wiederherstellung und Notfallwiederherstellung eingesetzt werden. Weitere Informationen dazu finden Sie in der Dokumentation des jeweiligen Anbieters.
- vSphere Data Protection, Site Recovery Manager und Symantec NetBackup. Weitere Informationen zu VMware BCDR-Lösungen finden Sie unter <http://www.vmware.com/business-continuity/business-continuity> und in der [VMware vCloud Suite-Dokumentation](#).
- Sicherungs-, Wiederherstellungs- und Notfallwiederherstellungsfunktion für Produkte, die in VMware vRealize® Log Insight integriert sind.
 - vRealize Operations Manager
 - vSphere Web Client-Server
 - ESXi-Hosts

Verwenden von statischen IP-Adressen und FQDN

Sie können statische IP-Adressen und FQDN verwenden, um während einer Sicherung, Wiederherstellung oder Notfallwiederherstellung Risiken zu vermeiden.

Statische IP-Adressen für vRealize Log Insight-Clusterknoten und den Lastausgleichsdienst

Wenn Sie statische IP-Adressen für alle Knoten in einem vRealize Log Insight-Cluster verwenden, müssen Sie die IP-Adressen der Clusterknoten nicht aktualisieren, wenn sich die IP-Adressen ändern.

vRealize Log Insight enthält alle Knoten-IP-Adressen jeder Konfigurationsdatei eines Clusterknotens wie im [Knowledgebase-Artikel 2123058](#) beschrieben.

Alle Produkte, die mit vRealize Log Insight (ESXi, vSphere, vRealize Operations) integriert werden können, verwenden den vollqualifizierten Domännennamen (FQDN) des Masterknotens des Clusters oder die IP-Adresse als syslog-Ziel. Diese Produkte könnten den FQDN oder die IP-Adresse des Lastausgleichsdienstes, sofern konfiguriert, als syslog-Ziel verwenden. Statische IP-Adressen reduzieren das Risiko, die Syslog-Ziel-IP-Adresse mehrerer Sites ständig aktualisieren zu müssen.

Geben Sie statische IP-Adressen und optionale virtuelle IP-Adressen für den Lastausgleichsdienst an. Bei der Konfiguration eines integrierten Lastausgleichsdienstes geben Sie den optionalen FQDN für die virtuelle IP-Adresse an. Der FQDN wird verwendet, wenn aus irgendeinem Grund eine IP-Adresse nicht erreichbar ist.

FQDN für vRealize Log Insight-Clusterknoten und Worker-Knoten

Wenn Sie einen FQDN für alle Knoten im vRealize Log Insight-Cluster verwenden, können Sie Zeit mit Konfigurationsänderungen nach einer Wiederherstellung sparen, sofern auf der Wiederherstellungs-Site derselbe FQDN aufgelöst werden kann.

Ein vollständig auflösbarer FQDN ist für den Masterknoten (Lastausgleichsdienst, falls verwendet) erforderlich. Andernfalls können die ESXi-Hosts die syslog-Meldungen nicht an vRealize Log Insight oder ein Remoteziel weiterleiten.

vRealize Log Insight verwendet für Systembenachrichtigungen FQDN-Hostnamen, sofern vorhanden, an Stelle von IP-Adressen.

Sie können davon ausgehen, dass sich nach Sicherungs- und Wiederherstellungs- oder Notfallwiederherstellungsvorgängen nur zugrunde liegende IP-Adressen ändern. Durch die Verwendung von FQDN entfällt die Notwendigkeit, die Syslog-Zieladresse (FQDN des Master-Knotens oder des internen Lastausgleichsdienstes) auf allen externen Geräten zu ändern, die Protokolle an den vRealize Log Insight-Cluster senden.

Überprüfen Sie, dass Anforderungen zum Beitreten von einem vRealize Log Insight-Worker-Knoten den FQDN des vRealize Log Insight-Masterknotens verwenden.

Der Hostwert für den Master-Knoten in der Konfigurationsdatei auf jedem Knoten basiert auf dem Wert, der vom ersten Worker-Knoten für das Senden einer Anforderung zum Beitreten verwendet wird. Wenn für die Anforderung zum Beitreten der FQDN des Master-Knotens verwendet wird, können nach der Notfallwiederherstellung keine manuellen Änderungen am Wert für den Host des Master-Knotens vorgenommen werden. Anderenfalls kann der Worker-Knoten dem Masterknoten erst dann erneut beitreten, wenn in den Konfigurationsdateien auf allen wiederhergestellten Clusterknoten der Hostname des Masterknotens aktualisiert wurde.

Planung und Vorbereitung

Lesen Sie vor dem Implementieren eines Vorgangs zur Sicherung, Wiederherstellung oder Notfallwiederherstellung die Informationen zur Planung und Vorbereitung in diesem Abschnitt.

Die folgenden Empfehlungen sollten in einen Sicherungs-, Wiederherstellungs- und Notfallwiederherstellungsplan aufgenommen werden.

Testen von Sicherungsvorgängen

Führen Sie einen Testlauf der Sicherungs-, Wiederherstellungs- und Notfallwiederherstellungsvorgänge in einer Test- oder Staging-Umgebung durch, bevor Sie diese Vorgänge live durchführen.

Führen Sie eine vollständige Sicherung des gesamten vRealize Log Insight-Clusters durch. Verlassen Sie sich nicht auf automatische Vorgänge zum Sichern von einzelnen Dateien und Konfigurationen.

Fehlerbehebungen überprüfen

Bevor Sie Sicherungs-, Wiederherstellungs- und Notfallwiederherstellungsvorgänge durchführen, stellen Sie sicher, dass alle Fehlerkorrekturen implementiert und die Ursachen von Warnungen und Fehlern behoben wurden. Sicherungs-, Wiederherstellungs- und Notfallwiederherstellungs-Tools bieten in der Regel visuelle Validierungen und Schritte, um sicherzugehen, dass die Sicherungs-, Wiederherstellungs- und Notfallwiederherstellungskonfigurationen ordnungsgemäß erstellt wurden.

Planen von Sicherungen

Je nach Clusterkonfiguration ist der erste Sicherungsvorgang in der Regel eine vollständige Sicherung. Sie sollten ausreichend Zeit für die erste Sicherung einplanen. Die nächsten Sicherungsvorgänge, bei denen es sich um inkrementelle oder vollständige Datensicherungen handeln kann, werden im Vergleich zum erstmaligen Sicherungsvorgang schneller durchgeführt.

Zusätzliche Dokumentation und Tools

Stellen Sie sicher, dass Sie Ressourcen für die Sicherungs-, Wiederherstellungs- und Notfallwiederherstellungs-Tools von vRealize Log Insight entsprechend der Dokumentation zuteilen.

Stellen Sie sicher, dass Sie die für Tools spezifischen Best Practices und Empfehlungen für Sicherungs-, Wiederherstellungs- und Notfallwiederherstellungs-Tools von Drittanbietern befolgen.

Verwenden Sie für virtuelle Maschinen, die mithilfe von VMware-Produkten bereitgestellt wurden, zusätzliche Tools, die spezielle Funktionen und Konfigurationen zum Unterstützen von Sicherungen, Wiederherstellungen und Notfallwiederherstellungen bieten.

Ereignisweiterleitungen und Cluster

Wenden Sie bei Ereignisweiterleitungen die Sicherungs-, Wiederherstellungs- und Notfallwiederherstellungsschritte für den vRealize Log Insight-Hauptcluster an. Weitere Informationen hierzu finden Sie unter [Wiederherstellen von Knoten und Clustern](#).

Basierend auf den Kundenanforderungen haben Sie möglicherweise eine oder mehrere vRealize Log Insight-Ereignisweiterleitungen. Darüber hinaus können die Ereignisweiterleitungen als Standalone-Knoten oder als Cluster installiert werden. Zum Zwecke der Sicherungs-, Wiederherstellungs- und Notfallwiederherstellungsvorgänge sind vRealize Log Insight-Ereignisweiterleitungen mit den primären vRealize Log Insight-Clusterknoten identisch und werden wie diese behandelt.

Sichern von Knoten und Clustern

Als Best Practice werden geplante Sicherungen oder Replizierungen für vRealize Log Insight-Knoten und Cluster eingerichtet.

vRealize Log Insight unterstützt keine Stilllegungs-Snapshots. Wenn Sie versuchen, einen stillgelegten Snapshot zu erstellen, wird dieser erstellt, die Stilllegung jedoch nicht angewendet. Weitere Informationen enthält der VMware Knowledge Base-Artikel [Virtuelle Log Insight-Appliance reagiert bei stillgelegten Snapshots nicht mehr](#).

Voraussetzungen

- Stellen Sie sicher, dass es keine Konfigurationsprobleme auf der Quell- und Ziel-Site gibt, bevor Sie den Sicherungs- bzw. Replizierungsvorgang durchführen.
- Stellen Sie sicher, dass die Zuteilung von Clusterressourcen nicht bei voller Kapazität ist.

Bei Konfigurationen mit angemessenen Ingestions- und Abfrageauslastungen ist es möglich, dass während Sicherungs- und Replizierungsvorgängen die Arbeitsspeicher- und Swap-Nutzung annähernd 100 % erreichen kann. Da der Arbeitsspeicher seine Kapazitätsgrenze in einer Live-Umgebung fast erreicht, ist die Arbeitsspeicherspitze zum Teil auf die vRealize Log Insight-Clusternutzung zurückzuführen. Außerdem können die geplanten Sicherungs- und Replizierungsvorgänge erheblich zur Arbeitsspeicherspitze beitragen.

1 3 In einigen Fällen werden die Worker-Knoten kurzzeitig für ein bis drei Minuten getrennt, bevor sie wieder dem Masterknoten beitreten, was an der hohen Arbeitsspeichernutzung liegen kann.

- Reduzieren Sie die Arbeitsspeicherdrosselung auf den vRealize Log Insight-Knoten, indem Sie eine der folgenden oder beide Maßnahmen durchführen:
 - Teilen Sie zusätzlichen Arbeitsspeicher über die von vRealize Log Insight empfohlenen Konfigurationen hinaus zu.
 - Planen Sie die wiederkehrenden Sicherungsvorgänge zu Zeiten außerhalb der Spitzenzeiten.

Vorgehensweise

- 1 Aktivieren Sie die regelmäßige Sicherung oder Replizierung von vRealize Log Insight-Ereignisweiterleitungen unter Verwendung derselben Verfahren wie beim vRealize Log Insight-Server.
- 2 Stellen Sie sicher, dass die Häufigkeit der Sicherungsvorgänge und die Sicherungstypen basierend auf den verfügbaren Ressourcen und den kundenspezifischen Anforderungen entsprechend ausgewählt werden.
- 3 Wenn Ressourcen kein Problem darstellen und dies vom Tool unterstützt wird, aktivieren Sie das gleichzeitige Sichern von Clusterknoten, um den Sicherungsvorgang zu beschleunigen.
- 4 Sichern Sie alle Knoten gleichzeitig.

Weiter

Überwachen – Während der Sicherungsvorgang läuft, achten Sie auf etwaige Umgebungs- und Leistungsprobleme im vRealize Log Insight-Setup. Die meisten Datensicherungs-, Wiederherstellungs- und Notfallwiederherstellungs-Tools stellen Überwachungsfunktionen zur Verfügung.

Überprüfen Sie während des Sicherungsvorgangs alle relevanten Protokolle auf dem Produktionssystem, da auf der Benutzeroberfläche möglicherweise nicht alle Probleme angezeigt werden.

Sichern von Linux- bzw. Windows-Agents

Sie sichern Agents, indem Sie die serverseitigen Installations- und Konfigurationsinformationen sichern. Eine gesonderte Sicherung des Agent-Knotens ist nicht erforderlich.

Agents werden meist auf Linux- oder Windows-Systemen installiert, die auch für weitere Anwendungen oder Services genutzt werden und in bestehende Sicherungen eingeschlossen sein können. Eine vollständige Sicherung des Computers auf Datei- oder Blockebene, die die gesamte Agent-Installation und die zugehörige Konfiguration umfasst, ist für die Wiederherstellung ausreichend. Agents unterstützen sowohl die lokale als auch die vom Server bereitgestellte Konfiguration.

Wenn der Agent ohne jede lokale Änderung der Konfigurationsdatei `liagent.ini` ausschließlich über den vRealize Log Insight-Server konfiguriert wird, müssen Sie keine Sicherung der Agent-Installation erstellen. Installieren Sie den Agent stattdessen neu und rufen Sie die Serversicherung ab.

Sofern es eine benutzerdefinierte lokale Konfiguration des Agent gibt, sichern Sie die Datei `liagent.ini`, stellen Sie diese wieder her und installieren Sie den Agent neu. Wenn Sie die Agent-Knoten für andere Aufgaben als das Installieren der Agent-Software verwenden und diese Knoten vollständig gesichert werden müssen, führen Sie die Datensicherung so durch, als würden Sie eine virtuelle Maschine sichern.

Wenn die Agent-Konfiguration clientseitig (auf den Agenten) durchgeführt wird und die Agent-Knoten nur verwendet werden, um die vRealize Log Insight Agent-Software zu installieren, reicht es aus, die Agent-Konfigurationsdatei zu sichern.

Voraussetzungen

Stellen Sie sicher, dass die Agent-Konfiguration sich auf vRealize Log Insight-Serverseite befindet.

Vorgehensweise

- 1 Sichern Sie die Datei `liagent.ini`.
- 2 Ersetzen Sie die Datei auf dem wiederhergestellten Agent oder der Linux- bzw. Windows-Maschine durch die gesicherte Datei.

Wiederherstellen von Knoten und Clustern

Knoten müssen in einer bestimmten Reihenfolge wiederhergestellt werden und bei einigen Wiederherstellungsszenarios sind möglicherweise manuelle Konfigurationsänderungen erforderlich.

Je nach Wiederherstellungs-Tool können die virtuellen Maschinen auf demselben Host, auf einem anderen Host in demselben Datencenter oder auf einem anderen Host in einem Remoteziel-Datencenter wiederhergestellt werden. Siehe [Ändern von Konfigurationen nach der Wiederherstellung](#).

Voraussetzungen

- Stellen Sie sicher, dass sich die wiederhergestellten Knoten im Zustand „Ausgeschaltet“ befinden.
- Stellen Sie sicher, dass die Clusterinstanzen ausgeschaltet sind, bevor Sie den Cluster auf einer neuen Site wiederherstellen.
- Stellen Sie sicher, dass es kein Split-Brain-Verhalten gibt, wenn dieselben IP-Adressen und FQDNs auf der Wiederherstellungs-Site verwendet werden.
- Stellen Sie sicher, dass niemand versehentlich einen teilweise funktionierenden Cluster auf der primären Site verwendet.

Vorgehensweise

- 1 Stellen Sie zuerst den Masterknoten wieder her, bevor Sie die Worker-Knoten wiederherstellen.
- 2 Die Worker-Knoten können in beliebiger Reihenfolge wiederhergestellt werden.

3 (Optional) Stellen Sie die Ereignisweiterleitungen wieder her, falls konfiguriert.

Stellen Sie sicher, dass der vRealize Log Insight Server (der Masterknoten und alle Worker-Knoten in einem Cluster-Setup) wiederhergestellt wird, bevor die Ereignisweiterleitung wiederhergestellt wird.

4 Stellen Sie wiederhergestellte Agenten wieder her.

Weiter

- Wenn dieselben IP-Adressen beim Wiederherstellen eines vRealize Log Insight-Clusters verwendet werden, stellen Sie sicher, dass die IP-Adressen und FQDNs aller wiederhergestellten Knoten den entsprechenden ursprünglichen Gegenstücken zugeordnet sind.

Das folgende Szenario schlägt beispielsweise fehl. Ein Cluster hat drei Knoten, A, B und C. Knoten A wird mit der IP-Adresse von B, Knoten B wird mit der IP-Adresse von C und Knoten C wird mit der IP-Adresse von A wiederhergestellt.

- Wenn dieselben IP-Adressen nur für einen Teil der wiederhergestellten Knoten verwendet werden, stellen Sie für diese Knoten sicher, dass alle wiederhergestellten Images ihren ursprünglichen IP-Adressen zugeordnet sind.
- Die meisten Sicherungs-, Wiederherstellungs- und Notfallwiederherstellungs-Tools bieten eine Art Überwachungsansicht, damit Sie den Fortschritt der Wiederherstellungsvorgänge auf Fehlschläge und Warnungen hin verfolgen können. Ergreifen Sie geeignete Maßnahmen zum Beheben erkannter Probleme.
- Falls manuelle Konfigurationsänderungen erforderlich sind, bevor die Site vollständig wiederhergestellt werden kann, halten Sie sich an die Richtlinien unter [Ändern von Konfigurationen nach der Wiederherstellung](#).
- Führen Sie nach einer erfolgreichen Wiederherstellung eine kurze Prüfung des wiederhergestellten Clusters durch.

Ändern von Konfigurationen nach der Wiederherstellung

Das während der Sicherungskonfiguration angewendete Wiederherstellungsziel und die IP-Anpassungen legen die erforderlichen manuellen Konfigurationsänderungen fest. Sie müssen Konfigurationsänderungen auf einen oder mehrere vRealize Log Insight-Knoten anwenden, damit die wiederhergestellte Site voll funktionsfähig werden kann.

Wiederherstellen auf demselben Host

Das Wiederherstellen eines vRealize Log Insight-Clusters auf demselben Host ist einfach und kann mit jedem Werkzeug durchgeführt werden.

Voraussetzungen

Lesen Sie wichtige Informationen zu [Planung und Vorbereitung](#).

Vorgehensweise

- 1 Schalten Sie vor Beginn des Wiederherstellungsvorgangs den vorhandenen Cluster aus.
Standardmäßig werden dieselben IP-Adressen und FQDNs für die wiederhergestellten Clusterknoten verwendet.
- 2 (Optional) Geben Sie einen neuen Namen für den Cluster an.

Während des Wiederherstellungsvorgangs wird die ursprüngliche Kopie des Clusters durch die wiederhergestellte Version überschrieben, es sei denn, es wird ein neuer Name für die virtuelle Maschine angegeben.
- 3 (Optional) Stellen Sie wenn möglich sicher, dass alle für die Produktionsumgebung verwendeten Netzwerk-, IP- und FQDN-Einstellungen auf der wiederhergestellten Site aufbewahrt werden.

Weiter

Löschen Sie nach einer erfolgreichen Wiederherstellung und einer erfolgreichen Plausibilitätsprüfung die alte Kopie, um Ressourcen zu schonen und mögliche versehentliche Split-Brain-Situationen zu verhindern, wenn ein Benutzer die alte Kopie einschaltet.

Wiederherstellen auf einem anderen Host

Wenn Sie auf einem anderen Host wiederherstellen, müssen Sie auf dem vRealize Log Insight-Cluster Konfigurationsänderungen vornehmen.

Ab vRealize Log Insight 3.0 und höheren Versionen wird das direkte Ändern der Konfigurationsdateien von der Appliance-Konsole aus nicht offiziell unterstützt. Informationen zur Durchführung dieser Änderungen mithilfe der Web-Benutzeroberfläche finden Sie im [Knowledgebase-Artikel 2123058](#).

Dies sind spezielle Konfigurationsänderungen für vRealize Log Insight-Builds, die für jedes Sicherungs- und Wiederherstellungs-Tool verwendet werden können.

Für das Wiederherstellen auf einem anderen Host sind manuelle Konfigurationsänderungen auf dem vRealize Log Insight-Cluster erforderlich. Sie können davon ausgehen, dass die wiederhergestellten vRealize Log Insight-Knoten über andere IP-Adressen und FQDNs als die entsprechenden Quellknoten verfügen, die gesichert wurden.

Voraussetzungen

Lesen Sie wichtige Informationen zu [Planung und Vorbereitung](#).

Vorgehensweise

- 1 Listen Sie alle neuen IP-Adressen und FQDNs auf, die jedem vRealize Log Insight-Knoten zugewiesen wurden.

- 2 Führen Sie die im Folgenden aufgeführten Konfigurationsänderungen auf dem Master-Knoten mithilfe der im [Knowledgebase-Artikel 2123058](#) beschriebenen Schritte durch.

- a Suchen Sie im Abschnitt „config“ von vRealize Log Insight nach Zeilen, die den im Folgenden aufgeführten Zeilen ähneln.

```
<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>
```

Der Code zeigt drei Knoten an. Der erste Knoten ist der Masterknoten, der `<service-group name=standalone>` zeigt, und die anderen beiden Knoten sind Worker-Knoten, die `<service-group name="workernode">` zeigen.

- b Prüfen Sie in der neu wiederhergestellten Umgebung für den Master-Knoten, ob der in der Umgebung vor der Wiederherstellung verwendete DNS-Eintrag wiederverwendet werden kann.
- Falls der DNS-Eintrag wiederverwendet werden kann, müssen Sie den DNS-Eintrag nur so aktualisieren, dass er auf die neue IP-Adresse des Masterknotens verweist.
 - Kann der DNS-Eintrag nicht wiederverwendet werden, ersetzen Sie den Eintrag für den Masterknoten durch einen neuen DNS-Namen (der auf die neue IP-Adresse verweist).
 - Falls der DNS-Name nicht zugewiesen werden kann, aktualisieren Sie als letzte Option den Konfigurationseintrag mit der neuen IP-Adresse.
- c Aktualisieren Sie zudem die IP-Adressen der Worker-Knoten entsprechend den neuen IP-Adressen.

- d Stellen Sie in derselben Konfigurationsdatei sicher, dass diese über Einträge verfügt, die NTP-, SMTP- sowie Datenbank- und „appender“-Abschnitte darstellen.

```
<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>
```

- Wenn in der neuen Umgebung die konfigurierten Werte des NTP-Servers nicht mehr gültig sind, passen Sie diese im Abschnitt `<ntp> . . . </ntp>` an.
 - Wenn in der neuen Umgebung die konfigurierten Werte des SMTP-Servers nicht mehr gültig sind, passen Sie diese im Abschnitt `<smtp> . . . </smtp>` an.
 - Optional können Sie auch den Wert für `default-sender` im SMTP-Abschnitt ändern. Es kann sich dabei um einen beliebigen Wert handeln, es wird jedoch empfohlen, einen Wert anzugeben, der die Quelle angibt, von wo aus die E-Mail gesendet wird.
 - Ändern Sie im Abschnitt `<database> . . . </database>` den Wert für den Host, so dass er auf den FQDN oder die IP-Adresse des Masterknotens verweist.
- e Aktualisieren Sie in derselben Konfigurationsdatei den vRealize Log Insight ILB-Konfigurationsabschnitt.

```
<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 Aktualisieren Sie im Abschnitt `<load-balancer> . . . </load-balancer>` den Wert `high-availability-ip`, wenn er sich von der aktuellen Einstellung unterscheidet.
- g Stellen Sie sicher, dass auch der FQDN des Lastausgleichsdienstes angepasst wird.

- h Führen Sie den Neustart über die Web-Benutzeroberfläche anhand der Registerkarte „Cluster“ auf der Seite „Verwaltung“ durch. Wählen Sie für jeden aufgeführten Knoten dessen Hostnamen oder IP-Adresse aus, um den Detailbereich zu öffnen, und klicken Sie auf **Log Insight neu starten**.

Die Konfigurationsänderungen werden automatisch auf alle Clusterknoten angewendet.

- i Warten Sie 2 Minuten nach dem Start des Dienstes vRealize Log Insight, damit für den Start des Cassandra-Dienstes ausreichend Zeit zur Verfügung steht, bevor andere Worker-Knoten online gestellt werden.

Weiter

Stellen Sie sicher, dass den wiederhergestellten vRealize Log Insight-Knoten andere IP-Adressen und FQDNs als den entsprechenden Quellknoten zugewiesen wurden, die gesichert wurden.


Überprüfen der Wiederherstellungen

Sie müssen sicherstellen, dass alle wiederhergestellten vRealize Log Insight-Cluster voll funktionsfähig sind.

Voraussetzungen

Bestätigen Sie, dass der Sicherungs- und Wiederherstellungsvorgang abgeschlossen ist, bevor Sie die Knoten- und Clusterkonfigurationen überprüfen.

Vorgehensweise

- 1 Melden Sie sich bei vRealize Log Insight mit der IP-Adresse oder dem FQDN (falls konfiguriert) des internen Lastenausgleichsdiensts (ILB) an.
- 2 Click the configuration drop-down menu icon  and select **Administration**.
- 3 Überprüfen Sie Folgendes:
 - a Stellen Sie sicher, dass Sie mit den entsprechenden IP-Adressen oder FQDNs auf alle einzelnen Clusterknoten zugreifen können.
 - b Verifizieren Sie den Status der Clusterknoten von der Clusterseite aus und stellen Sie sicher, dass sich der integrierte Lastenausgleichsdienst, sofern konfiguriert, im Zustand „Aktiv“ befindet.
 - c Prüfen Sie die vSphere-Integration. Falls erforderlich, konfigurieren Sie die Integration neu. Es ist eine Neukonfiguration erforderlich, wenn nach der Wiederherstellung die IP-Adresse bzw. der FQDN des Masterknotens und/oder des integrierten Lastenausgleichsdiensts geändert wird.
 - d Prüfen Sie die vRealize Operations Manager-Integration und konfigurieren Sie sie bei Bedarf neu.
 - e Stellen Sie sicher, dass alle Inhaltspakete und Funktionen der Benutzeroberfläche ordnungsgemäß funktionieren.
 - f Verifizieren Sie, dass die vRealize Log Insight-Ereignisweiterleitungen und -Agenten ordnungsgemäß funktionieren, sofern diese konfiguriert sind.

- 4 Stellen Sie sicher, dass die anderen wichtigen Funktionen von vRealize Log Insight wie erwartet funktionieren.

Weiter

Nehmen Sie an Ihrem Sicherungs- und Wiederherstellungsplan alle erforderlichen Änderungen vor, um Probleme zu beheben, die möglicherweise während der Sicherungs-, Wiederherstellungs- und Verifizierungsvorgänge identifiziert wurden.

Notfallwiederherstellung

Das Vorhandensein eines gut dokumentierten und getesteten Wiederherstellungsplans ist sehr wichtig, um den Cluster schnell wieder in einen funktionsfähigen Zustand zu versetzen.

Die Wahl des Replizierungstyps ist auch bei der Konfiguration einer virtuellen Maschine für die Notfallwiederherstellung entscheidend. Berücksichtigen Sie bei Ihrer Entscheidung für einen Replizierungstyp die Zielvorgaben für den Wiederanlaufpunkt (RPO), die Wiederanlaufzeit (RTO) sowie die Kosten und die Skalierbarkeit.

Bei dem Szenario einer Notfallwiederherstellung können Sie manchmal nicht auf derselben Site wiederherstellen, wenn die primäre Site vollständig ausgefallen ist. Abhängig von der ausgewählten Option sind einige manuelle Schritte erforderlich, um den vRealize Log Insight-Cluster vollständig wiederherzustellen und in den Zustand „Wird ausgeführt“ zu versetzen.

Solange der vRealize Log Insight-Cluster nicht vollständig ausgefallen ist und noch auf ihn zugegriffen werden kann, stellen Sie sicher, dass die Clusterinstanzen ausgeschaltet sind, bevor Sie den Cluster auf einer neuen Site wiederherstellen.

Stellen Sie bei einem Ausfall oder Notfall sobald wie möglich den vRealize Log Insight-Cluster wieder her.

Fehlerbehebung bei vRealize Log Insight

15

Bevor Sie sich an die VMware Support-Dienste wenden, können Sie allgemeine Probleme, die mit der Verwaltung von vRealize Log Insight in Zusammenhang stehen, selbst beheben.

Dieses Kapitel behandelt die folgenden Themen:

- [vRealize Log Insight steht zu wenig Festplattenspeicher zur Verfügung](#)
- [Scheitern des Imports archivierter Daten](#)
- [Erstellen eines Support-Pakets von vRealize Log Insight über die Virtual Appliance-Konsole](#)
- [Zurücksetzen des Admin-Benutzerkennworts](#)
- [Zurücksetzen des Root-Benutzerkennworts](#)
- [Warnungen konnten nicht an vRealize Operations Manager gesendet werden](#)
- [Anmeldung unter Verwendung der Active Directory-Anmeldedaten nicht möglich](#)
- [SMTP funktioniert bei aktivierter STARTTLS-Option nicht](#)
- [Fehlschlagen des Upgrades, weil die Signatur der PAK-Datei nicht validiert werden kann](#)
- [Fehlschlagen des Upgrades mit einem internen Serverfehler](#)

vRealize Log Insight steht zu wenig Festplattenspeicher zur Verfügung

Die Speicherkapazität eines vRealize Log Insight-Master- oder Worker-Knotens kann möglicherweise überschritten werden, wenn Sie eine kleine virtuelle Festplatte verwenden und keine Archivierung aktiviert ist.

Problem

vRealize Log Insight steht zu wenig Festplattenspeicher zur Verfügung, wenn der Anteil der eingehenden Protokolle 3 Prozent des Speicherplatzes pro Minute überschreitet.

Ursache

Im Normalfall wird die Speicherkapazität von vRealize Log Insight nie überschritten, da jede Minute geprüft wird, ob der freie Speicherplatz weniger als 3 Prozent beträgt. Wenn der freie Speicherplatz auf der virtuellen vRealize Log Insight-Appliance unter 3 Prozent fällt, werden alte Daten-Buckets stillgelegt.

Ist die Festplatte jedoch klein und die Protokollaufnahmerate so hoch, dass der freie Speicherplatz (3 Prozent) innerhalb von 1 Minute vollständig in Anspruch genommen wird, wird die Speicherkapazität von vRealize Log Insight überschritten.

Bei aktivierter Archivierung archiviert vRealize Log Insight das Bucket vor dessen Stilllegung. Wenn der freie Speicherplatz voll belegt ist, bevor das alte Bucket archiviert und stillgelegt wurde, steht vRealize Log Insight zu wenig Festplattenspeicher zur Verfügung.

Lösung

- ◆ Erhöhen Sie die Speicherkapazität der virtuellen vRealize Log Insight-Appliance. Weitere Informationen hierzu finden Sie unter [Erhöhen der Speicherkapazität der virtuellen vRealize Log Insight-Appliance](#).

Scheitern des Imports archivierter Daten

Der Import von archivierten Daten schlägt möglicherweise fehl, wenn in der virtuellen vRealize Log Insight-Appliance kein freier Speicherplatz verfügbar ist.

Problem

Das vRealize Log Insight-Repository-Importdienstprogramm überprüft nicht den verfügbaren Festplattenspeicher in der virtuellen vRealize Log Insight-Appliance. Deshalb schlägt der Import von archivierten Protokollen möglicherweise fehl, wenn für die virtuelle Appliance nicht ausreichend Speicherplatz verfügbar ist.

Lösung

Erhöhen Sie die Speicherkapazität der virtuellen vRealize Log Insight-Appliance und starten Sie den Importvorgang noch einmal. [Erhöhen der Speicherkapazität der virtuellen vRealize Log Insight-Appliance](#). Beachten Sie aber, dass die Informationen, die vor dem Fehler erfolgreich importiert wurden, dupliziert werden.

Erstellen eines Support-Pakets von vRealize Log Insight über die Virtual Appliance-Konsole

Wenn Sie nicht auf die Web-Benutzeroberfläche von vRealize Log Insight zugreifen können, können Sie mithilfe der Konsole der virtuellen Appliance oder nach Herstellung einer SSH-Verbindung zur virtuellen Appliance von vRealize Log Insight das Support-Paket herunterladen.

Voraussetzungen

- 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.

Vorgehensweise

- 1 Stellen Sie eine SSH-Verbindung zur vRealize Log Insight-vApp her und melden Sie sich als Root-Benutzer an.

- 2 Um das Support-Paket zu generieren, führen Sie `loginsight-support` aus.

Um ein Supportpaket zu generieren und nur Dateien aufzunehmen, die sich in einem bestimmten Zeitraum geändert haben, führen Sie den Befehl `loginsight-support` mit der Option `--days` aus. Beispielsweise werden mithilfe von `--days=1` nur Dateien aufgenommen, die sich in einem Tag geändert haben.

Die Support-Informationen werden erfasst und in einer `*.tar.gz`-Datei mit der folgenden Benennungskonvention gespeichert: `loginsight-support-YYYY-MM-DD_HHMMSS.xxxxx.tar.gz`, wobei `xxxxx` für die Prozess-ID steht, unter der der Prozess `loginsight-support` ausgeführt wurde.

Weiter

Leiten Sie das Support-Paket wie verlangt an die VMware Support-Dienste weiter.

Zurücksetzen des Admin-Benutzerkennworts

Wenn ein Admin-Benutzer das Kennwort für die Web-Benutzeroberfläche vergisst, ist das Konto nicht mehr erreichbar.

Problem

Wenn es nur einen Admin-Benutzer für vRealize Log Insight gibt und der Admin-Benutzer das Kennwort vergisst, kann die Anwendung nicht verwaltet werden. Wenn ein Admin-Benutzer der einzige Benutzer von vRealize Log Insight ist, kann auf die gesamte Web-Benutzeroberfläche nicht mehr zugegriffen werden.

Ursache

In vRealize Log Insight gibt es keine Benutzeroberfläche, in der Admin-Benutzer ihre eigenen Kennwörter zurücksetzen können, wenn ein Benutzer sich nicht an das aktuelle Kennwort erinnert.

Hinweis Admin-Benutzer, die sich anmelden können, können das Kennwort anderer Admin-Benutzer zurücksetzen. Setzen Sie das Admin-Benutzerkennwort nur zurück, wenn von allen Admin-Benutzerkonten kein Kennwort bekannt ist.

Lösung

Voraussetzungen

- Stellen Sie sicher, dass Sie über die Root-Benutzer-Anmeldedaten verfügen, um sich bei der virtuellen vRealize Log Insight-Appliance anzumelden. Siehe [SSH-Root-Kennwort für die virtuelle vRealize Log Insight-Appliance konfigurieren](#).
- Um SSH-Verbindungen zu aktivieren, überprüfen Sie zunächst, ob der TCP-Port 22 geöffnet ist.

Vorgehensweise

- 1 Stellen Sie eine SSH-Verbindung zur virtuellen vRealize Log Insight-Appliance her und melden Sie sich als Root-Benutzer an.

- 2 Geben Sie `li-reset-admin-passwd.sh` ein und drücken Sie die **Eingabetaste**.

Das Skript setzt das Admin-Benutzerkennwort zurück, erstellt ein neues Kennwort und zeigt dieses auf dem Bildschirm an.

Weiter

Melden Sie sich mit dem neuen Kennwort bei der Web-Benutzeroberfläche von vRealize Log Insight an und ändern Sie das Admin-Benutzerkennwort.

Zurücksetzen des Root-Benutzerkennworts

Wenn Sie das Kennwort des Root-Benutzers vergessen, können Sie keine SSH-Verbindungen mehr herstellen oder die Konsole der virtuellen vRealize Log Insight-Appliance verwenden.

Problem

Wenn Sie keine SSH-Verbindungen herstellen oder die Konsole der virtuellen vRealize Log Insight-Appliance nicht verwenden können, können Sie bestimmte Verwaltungsaufgaben nicht ausführen und das Kennwort des Admin-Benutzers nicht zurücksetzen.

Lösung

Es kann verschiedene Gründe dafür geben, dass Sie sich nicht als Root-Benutzer anmelden können, darunter:

- Sie haben das Standardkennwort nicht geändert. Standardmäßig legt vRealize Log Insight ein leeres Kennwort für den Root-Benutzer fest und deaktiviert den SSH-Zugriff. Nach Festlegen des Kennworts ist der SSH-Zugriff für den Root-Benutzer aktiviert.
- Sie legen einen SSH-Schlüssel während der Bereitstellung der virtuellen vRealize Log Insight-Appliance fest. Wenn ein SSH-Schlüssel über OVF angegeben wird, dann ist die Kennwortauthentifizierung deaktiviert. Melden Sie sich entweder mit dem festgelegten SSH-Schlüssel an, oder verwenden Sie die unten beschriebenen Lösungsschritte.
- Sie haben das Kennwort mehrmals falsch eingegeben und sind jetzt vorläufig gesperrt. In diesem Fall können Sie sich auch bei Eingabe des richtigen Kennworts nicht anmelden, bevor die Sperrzeit abgelaufen ist. Sie können entweder warten oder die virtuelle Appliance neu starten.

Vorgehensweise

- 1 Führen Sie im vSphere Client ein Herunterfahren des Gasts für die virtuelle vRealize Log Insight-Appliance durch.
- 2 Nach dem Herunterfahren der virtuellen Maschine wählen Sie **Einstellungen bearbeiten** aus.
- 3 Klicken Sie auf die Registerkarte **Optionen**.
- 4 Klicken Sie unter **vApp-Optionen** > **Erweitert** auf **Eigenschaften**.

5 Suchen und bearbeiten Sie den Schlüssel `vm.rootpw`.

Wenn Sie keinen Schlüssel `vm.rootpw` finden, fügen Sie einen neuen hinzu.

Wenn Sie SSH-Schlüssel anstelle der Kennwortauthentifizierung verwenden, dann bearbeiten Sie den Schlüssel `vm.sshkey` oder fügen ihn hinzu.

6 Geben Sie ein Kennwort ein.

Sie können hier stattdessen einen SSH-Schlüssel hinzufügen, wenn Sie nicht die Kennwortauthentifizierung verwenden.

7 Schalten Sie die virtuelle Appliance ein.

Weiter

Überprüfen Sie nach dem Start von vRealize Log Insight, dass Sie sich als Root-Benutzer anmelden können.

Warnungen konnten nicht an vRealize Operations Manager gesendet werden

vRealize Log Insight benachrichtigt Sie, wenn ein Warnungsereignis nicht an vRealize Operations Manager gesendet werden kann. vRealize Log Insight wiederholt das Senden der Warnung jede Minute, bis das Problem behoben ist.

Problem

In der Symbolleiste von vRealize Log Insight wird ein rotes Symbol mit einem Ausrufezeichen angezeigt, wenn eine Warnung nicht an vRealize Operations Manager übermittelt werden konnte.

Ursache

Aufgrund von Verbindungsproblemen kann vRealize Operations Manager vRealize Log Insight keine Warnungsbenachrichtigungen an vRealize Operations Manager versenden.

Lösung

- Klicken Sie auf das rote Symbol, um die Liste der Fehlermeldungen zu öffnen, und scrollen Sie nach unten, um die aktuellste Nachricht anzuzeigen.

Das rote Zeichen verschwindet von der Symbolleiste, wenn Sie die Liste der Fehlermeldungen öffnen oder das Problem behoben ist.
- Versuchen Sie, mit den folgenden Anweisungen das Verbindungsproblem mit vRealize Operations Manager zu beheben:
 - Stellen Sie sicher, dass die vRealize Operations Manager-vApp nicht heruntergefahren wurde.
 - Überprüfen Sie, ob Sie sich mit vRealize Operations Manager über die Schaltfläche **Verbindung testen** im Abschnitt **vRealize Operations Manager** der Seite **Verwaltung** der vRealize Log Insight-Web-Benutzeroberfläche verbinden können.

- Stellen Sie sicher, dass Sie über die richtigen Anmeldedaten verfügen, indem Sie sich direkt bei vRealize Operations Manager anmelden.
- Überprüfen Sie die Protokolle aus vRealize Log Insight und vRealize Operations Manager auf Meldungen, die auf Verbindungsprobleme hinweisen.
- Vergewissern Sie sich, dass keine Warnungen in der vRealize Operations Manager vSphere-Benutzeroberfläche herausgefiltert werden.

Anmeldung unter Verwendung der Active Directory-Anmeldedaten nicht möglich

Sie können sich nicht bei der Web-Benutzeroberfläche von vRealize Log Insight anmelden, wenn Sie Active Directory-Anmeldedaten verwenden.

Problem

Sie können sich nicht mit Ihren Anmeldedaten für die Active Directory-Domäne bei vRealize Log Insight anmelden, obwohl ein Administrator Ihr Active Directory-Konto in vRealize Log Insight aufgenommen hat.

Ursache

Die häufigsten Ursachen hierfür sind abgelaufene Kennwörter, falsche Anmeldedaten, Verbindungsprobleme oder mangelnde Uhrzeitsynchronisation zwischen der virtuellen vRealize Log Insight-Appliance und Active Directory.

Lösung

- Vergewissern Sie sich, dass Ihre Anmeldedaten gültig sind, Ihr Kennwort nicht abgelaufen und Ihr Active Directory-Konto nicht gesperrt ist.
- Wenn Sie keine Domäne zur Verwendung mit Active-Directory-Authentifizierung angegeben haben, stellen Sie sicher, dass Sie ein Konto auf der Standarddomäne haben, die in der neuesten vRealize Log Insight-Konfiguration unter `/storage/core/loginsight/config/loginsight-config.xml#[number]` gespeichert ist, wobei [Ziffer] die höchste Ziffer ist.
- Suchen Sie die neueste Konfigurationsdatei: `/storage/core/loginsight/config/loginsight-config.xml#[number]`, wobei [number] die höchste Ziffer ist.
- Stellen Sie sicher, dass vRealize Log Insight über eine Verbindung zum Active Directory-Server verfügt.
 - Begeben Sie sich zum **Authentifizierungsabschnitt** der **Verwaltungsseite** der vRealize Log Insight Web-Benutzeroberfläche, geben Sie Ihre Anmeldedaten ein und klicken Sie auf die Schaltfläche **Verbindung testen**.
 - Überprüfen Sie, ob in vRealize Log Insight `/storage/var/loginsight/runtime.log` mit DNS-Problemen verbundene Meldungen vorhanden sind.

- Stellen Sie sicher, dass die Uhrzeiten in vRealize Log Insight und Active Directory zueinander synchron sind.
 - Überprüfen Sie, ob in vRealize Log Insight `/storage/var/loginsight/runtime.log` mit Taktverschiebungen verbundene Meldungen vorhanden sind.
 - Verwenden Sie einen NTP-Server, um die Uhrzeiten von vRealize Log Insight und Active Directory zu synchronisieren.

SMTP funktioniert bei aktivierter STARTTLS-Option nicht

Bei der Konfiguration des SMTP-Servers mit aktivierter STARTTLS-Option schlägt der Versand von Test-E-Mails fehl. Fügen Sie Ihr SSL-Zertifikat für den SMTP-Server dem Java-Truststore hinzu, um das Problem zu beheben.

Voraussetzungen

- 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.

Vorgehensweise

- 1 Establish an SSH connection to the vRealize Log Insight vApp and log in as the root user.
- 2 Kopieren Sie das SSL-Zertifikat für den SMTP-Server in die vRealize Log Insight vApp.
- 3 Führen Sie den folgenden Befehl aus.

```
`/usr/java/latest/bin/keytool -import -alias zertifikat_name -file pfad_zum_zertifikat -
keystore /usr/java/latest/lib/security/cacerts`
```

Hinweis Die äußeren Anführungszeichen werden mit dem Gravis-Zeichen eingegeben, das sich auf Ihrer Tastatur auf derselben Taste befindet wie die Tilde. Verwenden Sie keine einfachen Anführungszeichen.

- 4 Geben Sie das Standardkennwort **changeit** ein.
- 5 Führen Sie den Befehl `service loginsight restart` aus.

Weiter

Gehen Sie auf **Verwaltung > Smtip** und testen Sie über **Test-E-Mail senden** Ihre Einstellungen. Siehe [Konfigurieren des SMTP-Servers für vRealize Log Insight](#).

Fehlschlagen des Upgrades, weil die Signatur der PAK-Datei nicht validiert werden kann

vRealize Log Insight-Upgrade schlägt aufgrund einer beschädigten PAK-Datei, einer abgelaufenen Lizenz oder nicht ausreichenden Festplattenspeichers fehl.

Problem

Das Upgrade von vRealize Log Insight schlägt fehl und die Fehlermeldung `Upgrade fehlgeschlagen`. Fehler beim Upgrade: Signatur der PAK-Datei kann nicht validiert werden wird angezeigt.

Ursache

Dieser Fehler kann die folgenden Ursachen haben:

- Bei der hochgeladenen Datei handelt es sich nicht um eine PAK-Datei.
- Die hochgeladene PAK-Datei ist nicht vollständig.
- Die Lizenz von vRealize Log Insight ist abgelaufen.
- Auf dem Root-Dateisystem der virtuellen vRealize Log Insight-Appliance ist nicht genügend Festplattenspeicher verfügbar.

Lösung

- Stellen Sie sicher, dass Sie eine PAK-Datei hochladen.
- Gleichen Sie „md5sum“ der PAK-Datei mit der VMware-Downloadsite ab.
- Stellen Sie sicher, dass mindestens eine gültige Lizenz für vRealize Log Insight konfiguriert ist.
- Melden Sie sich bei der virtuellen vRealize Log Insight-Appliance an und führen Sie `df -h` aus, um den verfügbaren Festplattenspeicher zu ermitteln.

Hinweis Legen Sie keine Dateien im Root-Dateisystem der virtuellen vRealize Log Insight-Appliance ab.

Fehlschlagen des Upgrades mit einem internen Serverfehler

Aufgrund eines Verbindungsproblems schlägt das vRealize Log Insight-Upgrade mit einem internen Serverfehler fehl.

Problem

Das Upgrade von vRealize Log Insight schlägt fehl und die Fehlermeldung `Upgrade fehlgeschlagen`. Interner Serverfehler wird angezeigt.

Ursache

Es ist ein Verbindungsproblem zwischen dem Client und dem Server aufgetreten. Dies geschieht beispielsweise, wenn Sie versuchen, ein Upgrade von einem Client auszuführen, welcher sich in einem WAN befindet.

Lösung

- ◆ Führen Sie das LI-Upgrade von einem Client in demselben LAN wie der Server aus.