# Erste Schritte

Update 1
Geändert am 3. September 2017
vRealize Log Insight 4.0

vmware®

Die neueste technische Dokumentation finden Sie auf der VMware-Website unter:

https://docs.vmware.com/de/

Auf der VMware-Website finden Sie auch die aktuellen Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com



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

**VMware Global, Inc.**
Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

# Inhalt

# Informationen zu „Erste Schritte in vRealize Log Insight “

„Erste Schritte in vRealize Log Insight“ enthält Informationen zur Bereitstellung und Konfiguration von VMware® vRealize™ Log Insight™. Dazu zählen Informationen zur Größenbestimmung der virtuellen vRealize Log Insight-Appliance für den Empfang von Protokollmeldungen aus einer Umgebung.

Diese Informationen helfen Ihnen bei der Planung und Installation Ihrer Bereitstellung. Dieses Handbuch wurde für erfahrene Linux- und Windows-Systemadministratoren verfasst, die mit der Technologie virtueller Maschinen sowie mit Datencenter-Vorgängen vertraut sind.

# Aktualisierte Informationen zu ersten Schritten

*Erste Schritte* für vRealize Log Insight wird mit jeder Produktversion oder bei Bedarf aktualisiert.

Diese Tabelle enthält den Update-Verlauf des Handbuchs *Erste Schritte* für vRealize Log Insight.

| Revision | Beschreibung |
|---|---|
| 002032-1 | ■ In dieser Revision wurden die Informationen zum Programm zur Verbesserung der Benutzerfreundlichkeit aktualisiert. Weitere Informationen hierzu finden Sie unter Kapitel 3, „Das Programm zur Verbesserung der Kundenzufriedenheit“, auf Seite 23.<br>■ In dieser Revision wurden die Themen zum Lebenszyklus eines Ereignisses überarbeitet. Siehe „Lebenszyklus eines Ereignisses“, auf Seite 14 und „Wichtige Aspekte des Ereignis-Lebenszyklus“, auf Seite 15. Beachten Sie, dass in Version 4.0 die maximale Größe für Gruppen auf 0.5 GB geändert wurde. |
| 002032 | Erstversion |

# Vor der Installation von vRealize Log Insight 1

Um mit der Nutzung von vRealize Log Insight in einer Umgebung zu beginnen, müssen die virtuelle vRealize Log Insight-Appliance bereitgestellt und mehrere grundlegende Konfigurationen angewendet werden.

Dieses Kapitel behandelt die folgenden Themen:



## In vRealize Log Insight unterstützte Protokolldateien und Archivformate

Sie können vRealize Log Insight zum Analysieren von unstrukturierten oder strukturierten Protokolldaten verwenden.

vRealize Log Insight akzeptiert Daten aus folgenden Quellen:

- Quellen, die das Senden von Protokoll-Streams mit dem Syslog-Protokoll unterstützen.
- Quellen, die Protokolldateien schreiben und den vRealize Log Insight-Agent ausführen können.
- Quellen, die Protokolldaten mit HTTP oder HTTPS mithilfe der REST API posten können. Weitere Informationen hierzu finden Sie unter https://www.vmware.com/go/loginsight/api.
- Historische Daten, die von vRealize Log Insight archiviert wurden

Der vSphere-Protokoll-Parser ermöglicht Ihnen, vSphere-Protokollpakete in vRealize Log Insight zu importieren.

**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.

Siehe Importieren eines Log Insight-Archivs in vRealize Log Insight unter *Verwalten von vRealize Log Insight*.

# Sicherheitsanforderungen

Zum Schutz Ihrer virtuellen Umgebung vor externen Angriffen sind bestimmte Regeln einzuhalten.

- Installieren Sie vRealize Log Insight stets in einem vertrauenswürdigen Netzwerk.
- Speichern Sie Support-Pakete für vRealize Log Insight stets an einem sicheren Ort.

IT-Entscheidungsträgern, -Architekten und -Administratoren sowie anderen Personen, die sich mit den Sicherheitskomponenten von vRealize Log Insight vertraut machen müssen, wird das Lesen der Sicherheitsthemen in *Verwalten von vRealize Log Insight* empfohlen.

Diese Themen enthalten detaillierte Informationen zu den Sicherheitsfunktionen von vRealize Log Insight. Zu den behandelten Themen gehören unter anderem die externen Schnittstellen, Ports und Authentifizierungsmechanismen sowie die Möglichkeiten zur Konfiguration und Verwaltung der Sicherheitsfunktionen.

Informationen zum Sichern Ihrer virtuellen Umgebung finden Sie im *VMware vSphere-Sicherheitshandbuch* sowie im Security Center auf der VMware-Website.

# Produktkompatibilität

vRealize Log Insight erfasst Daten anhand des Syslog-Protokolls und von HTTP, kann zur Erfassung von Ereignis-, Aufgaben- und Warnungsdaten die Verbindung mit vCenter Server herstellen und lässt sich zum Versand von Benachrichtigungsereignissen und Aktivieren des kontextbezogenen Starts in vRealize Operations Manager integrieren. Informationen zu den neuesten Updates für unterstützte Produktversionen enthalten die *Versionshinweise zu VMware vRealize Log Insight*.

## Bereitstellung der virtuellen Appliance

Die virtuelle vRealize Log Insight-Appliance muss mit Hilfe von vSphere bereitgestellt werden. Verwenden Sie stets einen vSphere-Client für die Verbindung mit einem vCenter Server. Die virtuelle vRealize Log Insight-Appliance sollte auf einem ESX/ESXi-Host der Version 4.1 oder höher bereitgestellt werden, der von vCenter Server 4.1 oder höher verwaltet wird.

## Syslog-Feeds

vRealize Log Insight erfasst und analysiert Syslog-Daten über die folgenden Ports und Protokolle:

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

Sie müssen Umgebungskomponenten wie Betriebssysteme, Anwendungen, Speicher, Firewalls und Netzwerkgeräte konfigurieren, um deren Syslog-Feeds an vRealize Log Insight zu senden.

## API-Feeds

Die vRealize Log Insight Ingestion-API erfasst Daten über den folgenden Port und das folgende Protokoll:

- 9000/TCP
- 9543/TCP (SSL)

## vSphere-Integration

Sie können vRealize Log Insight so konfigurieren, dass Daten zu Aufgaben, Ereignissen und Alarmen gesendet werden, die in einer oder mehreren Instanzen von vCenter Server auftreten. vRealize Log Insight nutzt die vSphere-API, um die Verbindung zu vCenter Server-Systemen herzustellen und Daten zu erfassen.

Sie können ESXi-Hosts zur Weiterleitung von Syslog-Daten an vRealize Log Insight konfigurieren.

Weitere Informationen zur Kompatibilität mit bestimmten Versionen von vCenter Server und ESXi finden Sie unter VMware-Produkt-Interoperabilitätstabellen

Weitere Informationen zur Verbindungsherstellung mit einer vSphere-Umgebung finden Sie unter Verbinden von vRealize Log Insight mit einer vSphere-Umgebung.

### vRealize Operations Manager-Integration

vRealize Log Insight und vRealize Operations Manager vApp oder Installable können auf zwei voneinander unabhängige Arten integriert werden.

Alle unterstützten Versionen von vCenter Operations Manager 6.0 und höher unterstützen Benachrichtigungen und kontextbezogenen Start.

- vRealize Log Insight kann Benachrichtigungsereignisse an vRealize Operations Manager senden.

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

- Das Menü für den kontextbezogenen Start von vRealize Operations Manager zeigt Aktionen in Verbindung mit vRealize Log Insight an.

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

## Mindestanforderungen

VMware verteilt vRealize Log Insight als eine virtuelle Appliance im OVA-Dateiformat. Verschiedene Ressourcen und Anwendungen müssen verfügbar sein, damit die virtuelle Appliance erfolgreich ausgeführt wird. Die neuesten Informationen über Anforderungen finden Sie in den aktuellen Versionshinweisen.

### Virtuelle Hardware

Während der Bereitstellung der virtuellen vRealize Log Insight-Appliance können Sie aus voreingestellten Konfigurationsgrößen gemäß der Aufnahmeanforderungen Ihrer Umgebung auswählen. Dabei handelt es sich um zertifizierte Größenkombinationen von Berechnungs- und Festplattenressourcen, anschließend können jedoch weitere Ressourcen hinzugefügt werden. Eine kleine Konfiguration, die in der folgenden Tabelle beschrieben ist, verbraucht bei bleibender Unterstützung die wenigsten Ressourcen. Es gibt auch eine extra kleine Konfiguration, diese ist jedoch nur für Demos geeignet.

Eine vollständige Auflistung der auf Aufnahmeanforderungen basierten Ressourcenanforderungen finden Sie unter „Dimensionierung der virtuellen vRealize Log Insight-Appliance“, auf Seite 13.

**Tabelle 1-1.** Voreingestellte Werte für die kleine Konfiguration

| Ressourcen | Mindestanforderung |
|---|---|
| Arbeitsspeicher | 8 GB |
| vCPU | 4 |
| Speicherplatz | 510 GB |

## Unterstützte Browser

Sie können einen der folgenden Browser verwenden, um eine Verbindung zur Web-Benutzeroberfläche von vRealize Log Insight herzustellen. Neuere Browserversionen funktionieren auch mit vRealize Log Insight, wurden aber bisher nicht validiert.

**Wichtig** Cookies müssen in Ihrem Browser aktiviert sein.

- Mozilla Firefox 45.0 und höher
- Google Chrome 51.0 und höher
- Safari 9.1 und höher
- Internet Explorer 11.0 und höher

**Hinweis** Der Internet Explorer-Dokumentmodus muss auf **Standard-Modus** festgelegt sein. Andere Modi werden nicht unterstützt. **Browser-Modus:** Die Kompatibilitätsansicht wird nicht unterstützt.

## Kontokennwörter

| Typ | Anforderungen |
|---|---|
| Stammordner | Die Standardanmeldedaten für den Root-Benutzer in der virtuellen vRealize Log Insight-Appliance lauten **root/<blank>**, es sei denn, Sie geben bei der OVA-Bereitstellung ein Root-Kennwort an oder verwenden die Gastanpassung. Sie werden dazu aufgefordert, beim ersten Zugriff auf die Konsole der virtuellen vRealize Log Insight-Appliance das Kennwort des Root-Kontos zu ändern.<br>**Hinweis** SSH wird erst aktiviert, wenn Sie das Root-Kennwort festgelegt haben. |
| Benutzerkonto | Mit vRealize Log Insight 3.3 oder höher erstellte Benutzerkonten müssen mit einem starken Kennwort versehen werden. Das Kennwort muss mindestens acht Zeichen mit mindestens einem Großbuchstaben, einem Kleinbuchstaben, einer Ziffer und einem Sonderzeichen enthalten. |

## Integrationsanforderungen

| Produkt | Anforderung |
|---|---|
| vCenter Server | Zum Abrufen von Daten zu Ereignissen, Aufgaben und Warnungen von einer vCenter Server-Instanz müssen Sie für diese vCenter Server-Instanz Benutzeranmeldedaten angeben. Zum Registrieren von bzw. zum Aufheben der Registrierung von vRealize Log Insight mit einem vCenter Server ist mindestens die Rolle **Nur Lesen** erforderlich. Sie muss auf vCenter Server-Ebene festgelegt werden und an die untergeordneten Objekte weitergegeben werden. Zum Konfigurieren von ESXi-Hosts, die ein vCenter Server verwaltet, benötigt vRealize Log Insight zusätzliche Rechte. |
| vSphere ESXi | vSphere ESXi 6.0 Update 1 oder höher ist erforderlich, um SSL-Verbindungen mit vRealize Log Insight herzustellen. |
| vRealize Operations Manager | Um Benachrichtigungsereignisse und die Funktion für den kontextbezogenen Start in einer vRealize Operations Manager-Instanz zu aktivieren, müssen Sie Benutzeranmeldedaten für diese vRealize Operations Manager-Instanz angeben. |

## Netzwerk-Portanforderungen

Auf die folgenden Netzwerkports muss extern zugegriffen werden können.

| Port | Protokoll |
|---|---|
| 80/TCP | HTTP |

| Port | Protokoll |
|---|---|
| 443/TCP | HTTPS |
| 514/UDP, 514/TCP | Syslog |
| 1514/TCP | Syslog |
| 9000/TCP | vRealize Log Insight Ingestion-API |
| 9543/TCP | vRealize Log Insight Ingestion-API (SSL) |

# Dimensionierung der virtuellen vRealize Log Insight -Appliance

Standardmäßig werden von der virtuellen vRealize Log Insight-Appliance die voreingestellten Werte für kleine Konfigurationen verwendet, bei denen 4 vCPUs, 8 GB virtueller Arbeitsspeicher und 510 GB Festplattenspeicher bereitgestellt werden. vRealize Log Insight verwendet 100 GB des Festplattenspeichers zur Speicherung von Raw-, Index- und Metadaten sowie anderen Informationen.

## Eigenständige Bereitstellung

Sie können die Einstellungen der Appliance ändern, um die Anforderungen der Umgebung zu erfüllen, für die Sie während der Bereitstellung Protokolle erfassen möchten.

vRealize Log Insight bietet voreingestellte VM-Größen, aus denen Sie auswählen können, um die Erfassungsanforderungen Ihrer Umgebung zu erfüllen. Dabei 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 geringsten Ressourcen. Eine extra kleine Konfiguration ist nur für Demos geeignet.

| Option | Protokollaufnahmerate | vCPUs | Arbeitsspeicher | IOPS | Syslog-Verbindungen | Ereignisse pro Sekunde |
|---|---|---|---|---|---|---|
| **Extra klein** | 6GB/Tag | 2 | 4 GB | 75 | 20 | 400 |
| **Klein** | 30GB/Tag | 4 | 8 GB | 500 | 100 | 2000 |
| **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.

Die Dimensionierung basiert auf den folgenden Annahmen:

- Jede vCPU weist mindestens 2 GHz auf.
- Jeder ESXi-Host sendet bis zu 10 Meldungen pro Sekunde mit einer Durchschnittsgröße von 170 Byte/Meldung. Dies entspricht ungefähr 150 MB/Tag/Host.

**Hinweis** Für umfangreiche Installationen ist ein Upgrade der virtuellen Hardwareversion der vRealize Log Insight-VM erforderlich. vRealize Log Insight unterstützt die virtuelle Hardwareversion 7 und höher. Die virtuelle Hardwareversion 7 unterstützt bis zu 8 vCPUs. Somit ist für ESXi 5.x ein Upgrade auf die virtuelle Hardwareversion 8 erforderlich, wenn Sie 16 vCPUs bereitstellen möchten. Mithilfe des vSphere-Clients können Sie ein Upgrade der virtuellen Hardware durchführen. Wenn Sie ein Upgrade der virtuellen Hardware auf die neueste Version durchführen möchten, informieren Sie sich entsprechend im VMware KB-Artikel Aktualisieren einer virtuellen Maschine auf die neueste Hardwareversion (1010675) .

### Cluster-Bereitstellung

Verwenden Sie eine mittelgroße oder größere Konfiguration für Master- und Worker-Knoten in einem vRealize Log Insight-Cluster. Die Anzahl der Ereignisse pro Sekunde nimmt linear mit der Anzahl der Knoten zu. Beispiel: In einem Cluster mit 3-12 Knoten (2 Knoten werden nicht unterstützt) beträgt die Nettoanzahl bei einem Cluster mit 12 Knoten 180.000 Ereignisse pro Sekunde (EPS) oder 2,7 TB an Ereignissen pro Tag.

### Reduzieren der Arbeitsspeichergröße

Wenn Sie die Version **Extra klein** der Appliance auf Ihrem Laptop verwenden möchten, dieser jedoch über unzureichenden Arbeitsspeicher verfügt, können Sie die Arbeitsspeichergröße auf 2 GB reduzieren.

## Integration von vRealize Log Insight und vRealize Operations Manager

Um die Integration zwischen vRealize Log Insight und vRealize Operations Manager zu ermöglichen, müssen beide Produkte entsprechend konfiguriert werden.

#### Vorgehensweise

1 Installieren Sie das vRealize Log Insight Management Pack in vRealize Operations Manager.

   Das vRealize Log Insight Management Pack wird für die Funktion „Kontextbezogener Start“ zwischen den beiden Produkten benötigt. Das vRealize Log Insight Management Pack ist im Download von vRealize Operations Manager oder auf der VMware Solution Exchange-Website erhältlich.

2 Konfigurieren Sie vRealize Log Insight für die Verbindung mit vRealize Operations Manager.

3 Konfigurieren Sie vRealize Log Insight-Warnungen so, dass sie Informationen an vRealize Operations Manager weiterleiten.

   Weitere Informationen finden Sie unter Konfigurieren von vRealize Log Insight zum Senden von Benachrichtigungsereignissen an vRealize Operations Manager in *Verwalten von vRealize Log Insight*.

4 Aktivieren Sie den kontextbezogenen Start in vRealize Operations, um Protokolle in vRealize Log Insight abzufragen.

   Weitere Informationen finden Sie unter Aktivieren des kontextbezogenen Starts für Log Insight in vRealize Operations Manager in *Verwalten von vRealize Log Insight*.

## Lebenszyklus eines Ereignisses

Der End-to-End-Lebenszyklus einer Protokollnachricht bzw. eines Protokollereignisses umfasst mehrere Stufen, während die Daten bei Agenten-Lese-, Analyse-, Aufnahme-, Indizierungs- (Buckets), Warnungs-, Abfrage-, Archivierungs- (Versiegeln und Weiterleiten von Buckets) und Löschvorgängen vRealize Log Insight durchlaufen.

Ein Ereignisübergang mit den folgenden Stufen.

1 Es wird auf einem Gerät generiert (außerhalb von vRealize Log Insight).

2 Es wird entnommen und auf eine der folgenden Arten an vRealize Log Insightgesendet (innerhalb und/oder außerhalb von vRealize Log Insight):

   - Über einen vRealize Log Insight-Agent unter Verwendung von Ingestion-API oder Syslog
   - Über einen Drittanbieter-Agent wie z. B. rsyslog, syslog-ng oder log4j unter Verwendung von Syslog
   - Per benutzerdefiniertes Schreiben in die Ingestion-API (z. B. log4j-Appender)

- Per benutzerdefiniertes Schreiben in Syslog (z. B. log4j-Appender)

3 vRealize Log Insight erhält das Ereignis.

- Wenn Sie den integrierten Lastausgleichsdienst (integrated Load Balancer, ILB) verwenden, wird das Ereignis an einen einzelnen Knoten weitergeleitet, der das Ereignis dann verarbeitet.
- Wird das Ereignis abgelehnt, verarbeitet der Client die Ablehnung als UDP-Löschung, TCP mit Protokolleinstellungen oder CFAPI mit festplattengesicherter Warteschlange.
- Wird das Ereignis akzeptiert, wird der Client benachrichtigt.

4 Das Ereignis durchläuft die vRealize Log Insight-Erfassungs-Pipeline, in der folgende Schritte erfolgen:

- Es wird ein Schlüsselwortindex erstellt oder aktualisiert. Der Index wird in einem proprietären Format auf der lokalen Festplatte gespeichert.
- Auf Clusterereignisse wird Maschinenlernen angewendet.
- Das Ereignis wird in einem komprimierten proprietären Format auf der lokalen Festplatte in einem Bucket gespeichert.

5 Das Ereignis wird abgefragt.

- Schlüsselwort- und glob-Abfragen werden mit dem Schlüsselwortindex abgeglichen
- Regex wird mit komprimierten Ereignissen abgeglichen

6 Das Ereignis wird archiviert.

- Bucket wird versiegelt und als archiviert markiert

7 Das Ereignis wird gelöscht.

- Buckets werden nach dem FIFO-Prinzip gelöscht.

# Wichtige Aspekte des Ereignis-Lebenszyklus

Mit der Fälligkeit von Ereignissen müssen Sie wichtige Punkte zur Ereignisspeicherung im Ereignis-Lebenszyklus berücksichtigen.

## Ereignisspeicher

Jedes Ereignis wird in einem einzelnen Bucket auf der Festplatte gespeichert. Beachten Sie bei der Verwendung von Buckets die folgenden Verhaltensweisen und Eigenschaften.

- Buckets können höchstens 0.5 GB groß sein. Erreicht ein Bucket 0.5 GB, wird er versiegelt und ist schreibgeschützt sowie zur Archivierung markiert. Nach der Archivierung wird ein versiegelter Bucket als archiviert markiert. Das bedeutet, dass ein Ereignis gleichzeitig sowohl lokal als auch in den Archiven aufbewahrt werden kann.
- Buckets werden in vRealize Log Insight nicht knotenübergreifend repliziert. Bei Verlust eines Knotens gehen auch die Daten an diesem Knoten verloren.
- Alle Buckets werden auf der Partition „/storage/core“ gespeichert.
- vRealize Log Insightlöscht alte Buckets, wenn auf der „/storage/core“-Partition weniger als 3 % Speicherplatz verfügbar sind. Buckets werden nach dem FIFO-Prinzip (First-in-first-out) gelöscht.

**Hinweis** Eine fast ausgeschöpfte „/storage/core“-Partition ist normal und wird erwartet. Diese Partition dürfte nie 100 % Kapazität erreichen, da vRealize Log Insight diese Partition verwaltet. Sie sollten allerdings nicht versuchen, Daten auf dieser Partition zu speichern, da dies das Löschen von alten Buckets beeinträchtigen könnte.

## Ereignisverwaltung

Beachten Sie die folgenden Merkmale und Verhaltensweisen von Ereignissen und Ereignisverwaltung in vRealize Log Insight.

- Nachdem ein Ereignis lokal gelöscht wurde, kann es nicht mehr abgefragt werden, es sei denn, es wird mithilfe der Befehlszeilenschnittstelle aus dem Archiv importiert.
- Nachdem alle Ereignisse für einen maschinenlernenden Cluster aus vRealize Log Insight gelöscht wurden, wird der Cluster entfernt.
- vRealize Log Insight verteilt alle eingehenden Ereignisse automatisch gleichmäßig auf die Knoten im Cluster. Wenn beispielsweise ein Ereignis explizit an einen bestimmten Knoten gesendet wird, kann es möglicherweise von einem anderen Knoten aufgenommen werden.
- Metadaten des Ereignisses werden in einem proprietären Format auf einem einzelnen vRealize Log Insight-Knoten und nicht in einer Datenbank gespeichert.
- Ein Ereignis kann sowohl lokal auf einem Knoten als auch im Archiv vorhanden sein.

# Installieren von vRealize Log Insight 2

vRealize Log Insight wird als virtuelle Appliance geliefert, die in Ihrer vSphere-Umgebung bereitgestellt werden muss.

Fahren Sie nach Durchsicht von „Dimensionierung der virtuellen vRealize Log Insight-Appliance“, auf Seite 13 mit „Bereitstellen der virtuellen vRealize Log Insight-Appliance“, auf Seite 17 fort. Folgen Sie sowohl für Einzelknoten- als auch für Clusterbereitstellungen dem in diesem Abschnitt beschriebenen standardmäßigen OVF-Bereitstellungsverfahren.

Dieses Kapitel behandelt die folgenden Themen:



## 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. Dabei 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 geringsten Ressourcen. Eine extra kleine Konfiguration ist nur für Demos geeignet.

| Option | Protokollaufnahmerate | vCPUs | Arbeitsspeicher | IOPS | Syslog-Verbindungen | Ereignisse pro Sekunde |
|---|---|---|---|---|---|---|
| **Extra klein** | 6GB/Tag | 2 | 4 GB | 75 | 20 | 400 |
| **Klein** | 30GB/Tag | 4 | 8 GB | 500 | 100 | 2000 |
| **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 zu einem späteren Zeitpunkt 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 Domänennamenserver an. Wenn Sie mehr als zwei Domänennamenserver angeben, werden alle konfigurierten Domänennamenserver in der virtuellen vRealize Log Insight-Appliance ignoriert.

Verwenden Sie eine kommagetrennte Liste, um Domänennamen 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“ 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.<br>a Schalten Sie die virtuelle vRealize Log Insight-Appliance aus.<br>b Klicken Sie mit der rechten Maustaste auf die virtuelle Appliance und wählen Sie **Einstellungen bearbeiten**.<br>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.

  Die vRealize Log Insight-Web-Benutzeroberfläche ist über https://*log-insight-host*/ verfügbar, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

## Starten einer neuen vRealize Log Insight-Bereitstellung

Beim erstmaligen Zugriff auf die Web-Benutzeroberfläche von vRealize Log Insight nach der Bereitstellung der virtuellen Appliance oder nach dem Entfernen eines Worker-Knotens aus einem Cluster müssen Sie die Schritte für die Erstkonfiguration ausführen.

Sämtliche Einstellungen, die Sie während der Erstkonfiguration ändern, stehen ebenfalls auf der Administrator-Web-Benutzeroberfläche zur Verfügung.

Informationen zu den Protokollierungsdaten, die von vRealize Log Insight erfasst und an VMware gesendet werden können, wenn Sie am Programm zur Verbesserung der Kundenzufriedenheit teilnehmen, finden Sie unter Kapitel 3, „Das Programm zur Verbesserung der Kundenzufriedenheit“, auf Seite 23.

### Voraussetzungen

- Notieren Sie sich die IP-Adresse der virtuellen vRealize Log Insight-Appliance in vSphere Client. Informationen zum Auffinden der IP-Adresse finden Sie unter „Bereitstellen der virtuellen vRealize Log Insight-Appliance“, auf Seite 17.
- Stellen Sie sicher, dass Sie einen unterstützten Browser verwenden. Weitere Informationen finden Sie unter „Mindestanforderungen“, auf Seite 11.
- Vergewissern Sie sich, dass Sie über einen gültigen Lizenzschlüssel verfügen. Sie können einen Test- oder permanenten Lizenzschlüssel über Ihr Konto in My VMware™ unter https://my.vmware.com/ anfordern.
- Wenn Sie lokale, vCenter Server- oder Active Directory-Anmeldedaten zur Integration von vRealize Log Insight mit vRealize Operations Manager verwenden möchten, vergewissern Sie sich, dass diese Benutzer in die benutzerdefinierte vRealize Operations Manager-Benutzeroberfläche importiert wurden. Weitere Informationen zur Konfiguration von LDAP finden Sie in der vRealize Operations Manager-Dokumentation.

### Vorgehensweise

1. Verwenden Sie einen unterstützten Browser, um zur Web-Benutzeroberfläche von vRealize Log Insight 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-Appliance ist.

   Der Erstkonfigurationsassistent wird geöffnet.
2. Klicken Sie auf **Neue Bereitstellung starten**.
3. Legen Sie das Kennwort für den Admin-Benutzer fest und klicken Sie auf **Speichern und fortfahren**.

   Optional können Sie eine E-Mail-Adresse für den Admin-Benutzer angeben.
4. Geben Sie den Lizenzschlüssel ein, klicken Sie auf **Lizenzschlüssel hinzufügen** und dann auf **Speichern und fortfahren**.
5. Geben Sie auf der allgemeinen Konfigurationsseite die E-Mail-Adresse ein, an die Systembenachrichtigungen von vRealize Log Insight gesendet werden sollen.
6. Wenn Sie Webhooks verwenden, um Benachrichtigungen an vRealize Operations oder eine Drittanbieteranwendung zu senden, geben Sie eine durch Leerzeichen getrennte Liste von URLs in das Feld **HTTP Post-Systembenachrichtigungen senden an** ein.
7. (Optional) Um das Programm zur Verbesserung der Benutzerfreundlichkeit zu verlassen, deaktivieren Sie das Kontrollkästchen **Am VMware-Programm zur Verbesserung der Benutzerfreundlichkeit teilnehmen**. Klicken Sie auf **Speichern und fortfahren**.
8. (Optional) Aktivieren Sie die Option **Immer Englisch verwenden**, damit die Benutzeroberfläche und der Inhalt stets in englischer Sprache angezeigt werden.

9 Legen Sie auf der Seite „Uhrzeitkonfiguration“ fest, wie die Uhrzeit auf der virtuellen vRealize Log Insight-Appliance synchronisiert werden soll, und klicken Sie auf **Testen**.

| Option | Beschreibung |
|---|---|
| **NTP-Server (empfohlen)** | Standardmäßig ist vRealize Log Insight für die Synchronisierung der Uhrzeit anhand von öffentlichen NTP-Servern konfiguriert. Kann auf einen externen NTP-Server aufgrund von Firewall-Einstellungen nicht zugegriffen werden, können Sie den internen NTP-Server in Ihrem Unternehmen heranziehen.<br>Verwenden Sie Kommas zum Trennen mehrerer NTP-Server. |
| **ESX/ESXi-Host** | Sind keine NTP-Server verfügbar, können Sie die Uhrzeit über den ESXi-Host synchronisieren, auf dem Sie die virtuelle vRealize Log Insight-Appliance bereitgestellt haben. |

10 Klicken Sie auf **Speichern und fortfahren**.

11 Legen Sie die Eigenschaften eines SMTP-Servers fest, um ausgehende Warnungen und Systembenachrichtigungs-E-Mails zu aktivieren.

Geben Sie zur Überprüfung der korrekten SMTP-Konfiguration eine gültige E-Mail-Adresse ein und klicken Sie auf **Testen**. vRealize Log Insight sendet daraufhin eine Test-E-Mail an die von Ihnen angegebene Adresse.

12 Klicken Sie auf **Speichern und fortfahren**.

Nach dem Neustart des vRealize Log Insight-Prozesses werden Sie zur Registerkarte **Dashboards** von vRealize Log Insight umgeleitet.

### Weiter

- Rufen Sie die Seite **Administration** durch Auswahl des Symbols im Dropdown-Menü in der Navigationsleiste auf und konfigurieren Sie vRealize Log Insight auf der Seite **vSphere-Integration** für das Abrufen von Aufgaben, Ereignissen und Warnungen aus vCenter Server-Instanzen sowie ESXi-Hosts zum Senden von Syslog-Feeds an vRealize Log Insight.

## 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. Dies ermöglicht eine lineare Skalierung des Aufnahmedurchsatzes, erhöht die Abfrageleistung und sorgt für Hochverfügbarkeit bei der Aufnahme. 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** Es wird nachdrücklich empfohlen, dass Sie in einem vRealize Log Insight-Cluster mindestens drei Knoten konfigurieren, um Aufnahme, Konfiguration und eine hohe Verfügbarkeit des Benutzerspeicherplatzes zu bieten.

### 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 Anfrage an den vRealize Log Insight-Master, der vorhandenen Bereitstellung beizutreten.

4 Klicken Sie auf den Link **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.

# Das Programm zur Verbesserung der Kundenzufriedenheit 3

Dieses Produkt nimmt am Programm zur Verbesserung der Kundenerfahrung („CEIP“) von VMware teil.

Details zur Datenerfassung über das CEIP-Programm und zur Verwendung der Daten durch VMware finden Sie im Trust & Assurance Center unter http://www.vmware.com/trustvmware/ceip.html. Zur Teilnahme am CEIP-Programm oder zum Verlassen des CEIP-Programms für dieses Produkt finden Sie Informationen unter „Teilnehmen oder Verlassen des VMware-Programms zur Verbesserung der Benutzerfreundlichkeit" in *Verwalten von vRealize Log Insight*.

# Index