

Installations- und Konfigurationshandbuch für vRealize Operations Manager für Linux und Windows

vRealize Operations Manager 6.4

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

Copyright © 2017 VMware, Inc. Alle Rechte vorbehalten. [Informationen zu Copyright und Marken.](#)

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

Grundlegendes zur Installation und Konfiguration für Linux und Windows	5
1 Vorbereitung für die Installation von vRealize Operations Manager	7
Komplexität Ihrer Umgebung	7
vRealize Operations Manager -Clusterknoten	10
Allgemeine Anforderungen an vRealize Operations Manager -Clusterknoten	10
Netzwerkanforderungen für vRealize Operations Manager -Clusterknoten	12
Best Practices für vRealize Operations Manager -Clusterknoten	13
Verwenden von IPv6 mit vRealize Operations Manager	14
Größenbestimmung des vRealize Operations Manager -Clusters	15
Angepasste vRealize Operations Manager -Zertifikate	16
Anforderungen für angepasste vRealize Operations Manager -Zertifikate	16
Beispielinhalte für angepasste vRealize Operations Manager -Zertifikate	17
Überprüfen eines angepassten vRealize Operations Manager -Zertifikats	19
2 Erstellen des vRealize Operations Manager -Master-Knotens	21
Über den vRealize Operations Manager -Master-Knoten	21
Ausführen des Setup-Assistenten zum Erstellen des Master-Knotens	21
3 Horizontales Skalieren von vRealize Operations Manager durch Hinzufügen eines Datenknotens	23
Über vRealize Operations Manager -Datenknoten	23
Ausführen des Setup-Assistenten zum Hinzufügen eines Datenknotens	24
4 Hinzufügen von High Availability zu vRealize Operations Manager	27
Über vRealize Operations Manager High Availability	27
Ausführen des Setup-Assistenten zum Hinzufügen eines Master-Replikationsknotens	28
5 Erfassen weiterer Daten durch Hinzufügen eines vRealize Operations Manager -Remote-Collector-Knotens	31
Über vRealize Operations Manager -Remote-Collector-Knoten	31
Ausführen des Setup-Assistenten zum Erstellen eines Remote Collector-Knotens	31
6 Fortfahren mit einer vRealize Operations Manager -Neuinstallation	33
Über vRealize Operations Manager -Neuinstallationen	33
Anmelden und Wiederaufnehmen einer Neuinstallation	33
7 Verbinden von vRealize Operations Manager mit Datenquellen	35
VMware vSphere Lösung in vRealize Operations Manager	35
Hinzufügen einer vCenter-Adapterinstanz in vRealize Operations Manager	37
Konfigurieren des Benutzerzugriffs für Aktionen	38

Endpoint Operations Management Lösung in vRealize Operations Manager	39
Installation und Bereitstellung des Endpoint Operations Management -Agenten	39
Rollen und Berechtigungen in vRealize Operations Manager	78
Registrieren von Agenten auf Clustern	78
Manuelles Erstellen von Betriebssystemobjekten	79
Verwalten von Objekten mit fehlenden Konfigurationsparametern	80
Zuordnen virtueller Maschinen zu Betriebssystemen	81
Installieren optionaler Lösungen in vRealize Operations Manager	81
Verwalten der Anmeldedaten für Lösungen	82
Verwalten von Collector-Gruppen	83
Migrieren einer vCenter Operations Manager-Bereitstellung in diese Version	83
8 Überlegungen nach der Installation von vRealize Operations Manager	85
Grundlegendes zum Anmelden bei vRealize Operations Manager	85
Das Programm zur Verbesserung der Kundenerfahrung	86
Teilnahme am Programm zur Verbesserung der Kundenerfahrung für	
vRealize Operations Manager oder Verlassen des Programms	86
9 Aktualisieren Ihrer Software	87
Ermitteln der PAK-Datei für das Software-Update	87
Erstellen eines Snapshots im Rahmen eines Updates	88
Installieren eines Software-Updates	89
Index	91

Grundlegendes zur Installation und Konfiguration für Linux und Windows

Das *vRealize Operations Manager Installations- und Konfigurationshandbuch für Linux und Windows* bietet Informationen über das Installieren von VMware® vRealize Operations Manager unter Linux und Windows, einschließlich Informationen darüber, wie der vRealize Operations Manager-Cluster erstellt und konfiguriert wird.

Der vRealize Operations Manager-Installationsvorgang besteht aus dem Ausführen des vRealize Operations Manager Enterprise-Installationsprogramms auf jedem Clusterknoten und dem Zugriff auf das Produkt, um das Einrichten der Anwendung abzuschließen.

Zielgruppe

Diese Informationen sind für Personen bestimmt, die vRealize Operations Manager auf Linux- oder Windows-Maschinen installieren und konfigurieren möchten. Die Informationen sind für erfahrene Linux- bzw. Windows-Systemadministratoren bestimmt, die mit den Enterprise Management-Anwendungen und Datacenter-Vorgängen vertraut sind.

VMware Technical Publications - Glossar

VMware Technical Publications enthält ein Glossar mit Begriffen, die Ihnen möglicherweise unbekannt sind. Definitionen von Begriffen, die in der technischen Dokumentation von VMware verwendet werden, finden Sie unter <http://www.vmware.com/support/pubs>.

Vorbereitung für die Installation von vRealize Operations Manager

1

Die Vorbereitung für die Installation von vRealize Operations Manager erfolgt in Form einer Bewertung Ihrer Umgebung und der Bereitstellung von einer ausreichenden Anzahl von vRealize Operations Manager-Clusterknoten, um den gewünschten Einsatz des Produkts zu unterstützen.

Dieses Kapitel behandelt die folgenden Themen:

- „Komplexität Ihrer Umgebung“, auf Seite 7
- „vRealize Operations Manager-Clusterknoten“, auf Seite 10
- „Verwenden von IPv6 mit vRealize Operations Manager“, auf Seite 14
- „Größenbestimmung des vRealize Operations Manager-Clusters“, auf Seite 15
- „Angepasste vRealize Operations Manager-Zertifikate“, auf Seite 16

Komplexität Ihrer Umgebung

Wenn Sie vRealize Operations Manager bereitstellen, sind die Anzahl und die Art der zu überwachenden Objekte möglicherweise so komplex, dass die Mitwirkung der Professional Services in Betracht zu ziehen ist.

Komplexitätsebenen

Unternehmen unterscheiden sich darin, was die vorhandenen Systeme und die Erfahrung des Personals bei der Bereitstellung angeht. Die folgende farbcodierte Tabelle soll Ihnen dabei helfen, Ihre Komplexität zu ermitteln.

■ Grün

Ihre Installation enthält nur Bedingungen, die die meisten Benutzer ohne Hilfe verstehen und mit denen sie arbeiten können. Fahren Sie mit der Bereitstellung fort.

■ Gelb

Ihre Installation enthält Bedingungen, die abhängig von Ihrem Kenntnisstand Hilfe bei der Bereitstellung erfordern können. Bevor Sie fortfahren, sollten Sie sich an Ihren Kundenbeauftragten wenden und mit diesem die Mitwirkung der Professional Services abwägen.

■ Rot

Ihre Installation enthält Bedingungen, für die die Mitwirkung der Professional Services sehr empfehlenswert ist. Bevor Sie fortfahren, sollten Sie sich an Ihren Kundenbeauftragten wenden und mit diesem die Mitwirkung der Professional Services abwägen.

Beachten Sie, dass diese farbcodierten Ebenen keine festen Regeln sind. Ihre Produkterfahrung, die sich durch die Nutzung von vRealize Operations Manager und die Partnerschaft mit Professional Services erhöht, muss bei der Bereitstellung von vRealize Operations Manager berücksichtigt werden.

Tabelle 1-1. Auswirkung der Bereitstellungsbedingungen auf die Komplexität

Komplexitätsebene	Aktuelle oder neue Bereitstellungsbedingung	Zusätzliche Hinweise
Grün	Sie führen nur eine vRealize Operations Manager-Bereitstellung aus.	Einzelne Instanzen können in vRealize Operations Manager in der Regel einfach erstellt werden.
Grün	Ihre Bereitstellung enthält ein Management Pack, das gemäß dem Kompatibilitätshandbuch auf der VMware Solutions Exchange -Website als Grün aufgelistet ist.	Das Kompatibilitätshandbuch führt auf, ob das unterstützte Management Pack für vRealize Operations Manager ein kompatibles 5.x-Pack oder ein neues Pack für diese Version ist. In einigen Fällen funktionieren möglicherweise beide Varianten, führen aber zu unterschiedlichen Ergebnissen. Ungeachtet dessen benötigen die Benutzer möglicherweise Hilfestellung beim Anpassen der Konfiguration, damit die zugewiesenen Daten, Dashboards, Warnungen usw. wie erwartet angezeigt werden. Beachten Sie, dass die Begriffe <i>Lösung</i> , <i>Management Pack</i> , <i>Adapter</i> und <i>Plug-in</i> austauschbar sind.
Gelb	Sie führen mehrere Instanzen von vRealize Operations Manager aus.	Mehrere Instanzen dienen in der Regel dazu, um Muster bei der Skalierung oder Bedienernutzung zu behandeln.
Gelb	Ihre Bereitstellung enthält ein Management Pack, das gemäß dem Kompatibilitätshandbuch auf der VMware Solutions Exchange -Website als Gelb aufgelistet ist.	Das Kompatibilitätshandbuch führt auf, ob das unterstützte Management Pack für vRealize Operations Manager ein kompatibles 5.x-Pack oder ein neues Pack für diese Version ist. In einigen Fällen funktionieren möglicherweise beide Varianten, führen aber zu unterschiedlichen Ergebnissen. Ungeachtet dessen benötigen die Benutzer möglicherweise Hilfestellung beim Anpassen der Konfiguration, damit die zugewiesenen Daten, Dashboards, Warnungen usw. wie erwartet angezeigt werden.
Gelb	Sie stellen Remote Collector-Knoten von vRealize Operations Manager bereit.	Remote Collector-Knoten erfassen Daten, überlassen das Speichern und Verarbeiten der Daten aber dem Analyse-Cluster.
Gelb	Sie stellen einen vRealize Operations Manager-Cluster mit mehreren Knoten bereit.	Mehrere Knoten werden in der Regel für die horizontale Skalierung der Überwachungsfunktionalität von vRealize Operations Manager verwendet.
Gelb	Ihre neue vRealize Operations Manager-Instanz enthält eine Linux- oder Windows-basierende Bereitstellung.	Linux- und Windows-Bereitstellungen sind weniger häufig als vApp-Bereitstellungen. Für sie müssen oft spezielle Überlegungen angestellt werden.

Tabelle 1-1. Auswirkung der Bereitstellungsbedingungen auf die Komplexität (Fortsetzung)

Komplexitätsebene	Aktuelle oder neue Bereitstellungsbedingung	Zusätzliche Hinweise
Gelb	Ihre vRealize Operations Manager-Instanz verwendet High Availability (HA).	High Availability und das dazugehörige Knoten-Failover ist eine einzigartige Mehrknotenfunktion, zu deren Verständnis Sie Hilfestellung in Anspruch nehmen können.
Gelb	Sie erhalten auch Unterstützung, falls Sie Hilfe zu den neuen und geänderten Funktionen in vRealize Operations Manager benötigen und wie diese in Ihrer Umgebung verwendet werden.	vRealize Operations Manager unterscheidet sich von vCenter Operations Manager bei den Richtlinien, den Warnungen, der Übereinstimmung, den benutzerdefinierten Berichten und den Badges. Außerdem verwendet vRealize Operations Manager eine konsolidierte Schnittstelle.
Rot	Sie führen mehrere Instanzen von vRealize Operations Manager aus, wobei mindestens eine Instanz eine Virtual Desktop Infrastructure (VDI) enthält.	Mehrere Instanzen dienen in der Regel dazu, Muster bei der Skalierung oder der Bedienernutzung zu behandeln, oder weil separate VDI- (V4V-Überwachung) und Nicht-VDI-Instanzen benötigt werden.
Rot	Ihre Bereitstellung enthält ein Management Pack, das gemäß dem Kompatibilitätshandbuch auf der VMware Solutions Exchange -Website als Rot aufgelistet ist.	Das Kompatibilitätshandbuch führt auf, ob das unterstützte Management Pack für vRealize Operations Manager ein kompatibles 5.x-Pack oder ein neues Pack für diese Version ist. In einigen Fällen funktionieren möglicherweise beide Varianten, führen aber zu unterschiedlichen Ergebnissen. Ungeachtet dessen benötigen die Benutzer möglicherweise Hilfestellung beim Anpassen der Konfiguration, damit die zugewiesenen Daten, Dashboards, Warnungen usw. wie erwartet angezeigt werden.
Rot	Sie stellen mehrere vRealize Operations Manager-Cluster bereit.	Mehrere Cluster dienen in der Regel zum Isolieren von Geschäftsvorgängen oder Funktionen.
Rot	Ihre aktuelle vRealize Operations Manager-Bereitstellung erforderte für die Installation die Mitwirkung der Professional Services.	Falls Ihre Umgebung so komplex war, dass der Einsatz der Professional Services in der Vorgängerversion erforderlich war, ist es möglich, dass diese Bedingungen immer noch vorliegen und ein ähnliches Mitwirken auch in dieser Version nahelegen.
Rot	Ihre vRealize Operations Manager-Bereitstellung wurde durch Professional Services angepasst. Beispiele für Anpassungen sind spezielle Integrationen, Skripting, nicht standardmäßige Konfigurationen, mehrere Warnebenen oder benutzerdefinierte Berichte.	Falls Ihre Umgebung so komplex war, dass der Einsatz der Professional Services in der Vorgängerversion erforderlich war, ist es möglich, dass diese Bedingungen immer noch vorliegen und ein ähnliches Mitwirken auch in dieser Version nahelegen.

vRealize Operations Manager -Clusterknoten

Alle vRealize Operations Manager-Cluster bestehen aus einem Master-Knoten, einem optionalen Replikationsknoten für High Availability, optionalen Datenknoten und optionalen Remote-Collector-Knoten.

Wenn Sie vRealize Operations Manager installieren, verwenden Sie eine vRealize Operations Manager-vApp-Bereitstellung, ein Linux-Installationsprogramm oder ein Windows-Installationsprogramm, um Knoten ohne Rolle zu erstellen. Nachdem die Knoten erstellt wurden und ihre Namen und IP-Adressen erhalten haben, verwenden Sie eine Verwaltungsschnittstelle, um sie entsprechend ihren Rollen zu konfigurieren.

Sie erstellen alle Knoten ohne Rolle auf einmal oder nach Bedarf. In der Praxis werden Knoten nach Bedarf hinzugefügt, wenn Sie vRealize Operations Manager horizontal skalieren, um eine größer werdende Umgebung zu überwachen.

Das vRealize Operations Manager-Analyse-Cluster besteht aus den folgenden Knotentypen:

Master-Knoten	<p>Der erste erforderliche Knoten im vRealize Operations Manager. Alle anderen Knoten werden durch den Master-Knoten verwaltet.</p> <p>Bei einer Einzelknoteninstallation verwaltet sich der Master-Knoten selbst. Auf ihm sind Adapter installiert und er führt die gesamte Datenerfassung und -analyse durch.</p>
Datenknoten	<p>Bei größeren Bereitstellungen sind bei den zusätzlichen Datenknoten Adapter installiert, welche die Erfassung und Analyse der Daten durchführen.</p> <p>Größere Bereitstellungen umfassen normalerweise nur Adapter an den Datenknoten, sodass die Master- und Replikationsknotenressourcen für die Clusterverwaltung eingesetzt werden können.</p>
Replikationsknoten	<p>Um vRealize Operations Manager-High Availability (HA) zu verwenden, erfordert der Cluster, dass Sie einen Datenknoten in eine Replikation des Master-Knotens umwandeln.</p>

Der folgende Knotentyp ist ein Mitglied des vRealize Operations Manager-Clusters, jedoch nicht Teil des Analyse-Clusters:

Remote-Collector-Knoten	<p>Verteilte Bereitstellungen erfordern gegebenenfalls einen Remote-Collector-Knoten, der über Firewalls navigieren, eine Schnittstelle mit einer Remote-Datenquelle herstellen, Bandbreitenbedarf zwischen Rechenzentren reduzieren oder die Arbeitslast für den vRealize Operations Manager-Analyse-Cluster reduzieren kann. Remote Collectors erfassen Objekte nur für den Bestand, ohne Daten zu speichern oder Analysen durchzuführen. Außerdem können Remote-Collector-Knoten auf einem anderen Betriebssystem installiert werden als der Rest des Clusters.</p>
--------------------------------	--

Allgemeine Anforderungen an vRealize Operations Manager -Clusterknoten

Wenn Sie die Clusterknoten erstellen, aus denen der vRealize Operations Manager besteht, müssen allgemeine Anforderungen erfüllt werden.

Allgemeine Anforderungen

- vRealize Operations Manager Version. Alle Knoten müssen mit derselben vRealize Operations Manager-Version laufen.

Fügen Sie zum Beispiel keinen Datenknoten mit Version 6.1 zum einem Cluster mit vRealize Operations Manager 6.2-Knoten hinzu.

- Bereitstellungstyp des Analyse-Clusters. Im Analyse-Cluster müssen alle Knoten dieselbe Art der Bereitstellung haben: vApp, Linux oder Windows.

Vermischen Sie nicht vApp-, Linux- und Windows-Knoten in demselben Analysecluster.

- Bereitstellungstyp des Remote-Controllers. Ein Remote-Controller-Knoten muss nicht denselben Bereitstellungstyp haben wie die Analyse-Clusterknoten.

Wenn Sie einen Remote Collector mit einer anderen Bereitstellungsart hinzufügen, werden folgende Kombinationen unterstützt:

- vApp-Analyse-Cluster und Windows Remote Collector
- Linux-Analyse-Cluster und Windows Remote Collector

- Größe des Analyse-Clusterknotens. Im Analyse-Cluster müssen CPU, Arbeitsspeicher und Festplattengröße für alle Knoten identisch sein.

Master-, Replik- und Datenknoten müssen eine einheitliche Größe aufweisen.

- Größe des Remote-Collector-Knotens. Remote-Collector-Knoten müssen keine einheitliche Größe haben und können eine andere Größe aufweisen als die einheitlichen Analyse-Clusterknoten.

- Geografische Entfernung. Sie können Analyse-Clusterknoten in unterschiedliche vSphere-Cluster platzieren, aber die Knoten müssen sich an demselben geografischen Ort befinden.

Abweichende geografische Standorte werden nicht unterstützt.

- Wartung der virtuellen Maschine. Wenn ein Knoten eine virtuelle Maschine ist, können Sie die Software der virtuellen Maschine nur aktualisieren, indem Sie die vRealize Operations Manager-Software direkt aktualisieren.

Folgendes wird beispielsweise nicht unterstützt: Von außerhalb von vRealize Operations Manager auf vSphere zuzugreifen, um VMware Tools zu aktualisieren.

- Redundanz und Isolierung. Wenn Sie eventuell HA aktivieren wollen, platzieren Sie die Analyse-Clusterknoten auf separaten Hosts. Weitere Informationen hierzu finden Sie unter „Über vRealize Operations Manager High Availability“, auf Seite 27.

Anforderungen für Lösungen

Beachten Sie, dass Lösungen Anforderungen über jene für den vRealize Operations Manager hinaus haben können. So hat beispielsweise vRealize Operations Manager für Horizon View spezielle Größenrichtlinien für seine Remote-Collectoren.

Lesen Sie in Ihrer Lösungsdokumentation nach und prüfen Sie alle weiteren Anforderungen, bevor Sie Lösungen installieren. Beachten Sie, dass die Begriffe *Lösung*, *Management Pack*, *Adapter* und *Plug-In* austauschbar sind.

Netzwerkanforderungen für vRealize Operations Manager -Clusterknoten

Wenn Sie die Clusterknoten erstellen, aus denen der vRealize Operations Manager besteht, ist die damit verbundene Konfiguration in Ihrer Netzwerkumgebung wichtig für die Kommunikation zwischen den Knoten und für den korrekten Betrieb.

Netzwerkanforderungen

WICHTIG vRealize Operations Manager-Analyse-Clusterknoten müssen häufig miteinander kommunizieren. Im Allgemeinen schafft Ihre zugrunde liegende vSphere-Architektur Bedingungen, aufgrund derer sich einige vSphere-Aktionen auf diese Kommunikation auswirken können. Beispiele sind unter anderem vMotions, Storage vMotions, HA-Ereignisse und DRS-Ereignisse.

- Die Master- und Replikatknoten müssen statische IP-Adressen oder einen vollqualifizierten Domänennamen (FQDN – Fully Qualified Domain Name) mit einer statischen IP-Adresse haben.
Daten- und Remote-Collector-Knoten können DHCP (Dynamic Host Control Protocol) verwenden.
- Sie können alle Knoten, einschließlich Remote-Collectors, einem Reverse-DNS lookup zu ihrem FQDN, aktuell dem Knoten-Hostnamen, unterziehen.
Bei über OVF bereitgestellten Knoten werden ihre Hostnamen standardmäßig auf den abgerufenen FQDN gesetzt.
- Alle Knoten, einschließlich Remote-Collectors, müssen per IP-Adresse oder FQDN bidirektional routingfähig sein.
- Trennen Sie nicht die Analyse-Clusterknoten mit NAT (Network Address Translation), Load Balancer (Lastausgleichsdienst), Firewall oder mit einem Proxy, der/das bidirektionale Kommunikation per IP-Adresse oder FQDN unterbindet.
- Analyse-Clusterknoten dürfen nicht denselben Hostnamen haben.
- Platzieren Sie Analyse-Clusterknoten in demselben Rechenzentrum und verbinden Sie sie mit demselben LAN (Local Area Network).
- Platzieren Sie Analyse-Clusterknoten auf demselben Layer-2-Netzwerk und IP-Subnetz.
Ein gestrecktes Layer-2- oder geroutetes Layer-3-Netzwerk wird nicht unterstützt.
- Spannen Sie das Layer-2-Netzwerk nicht über Standorte hinweg, da dies zu Netzwerkpartitionen oder Netzwerkproblemen führen kann.
- Die Einwege-Latenz zwischen Analyse-Clusterknoten muss 5 ms betragen oder geringer sein.
- Die Netzwerkbandbreite zwischen Analyse-Clusterknoten muss 1 Gbit/s oder höher sein.
- Verteilen Sie Analyse-Clusterknoten nicht über ein WAN (Wide Area Network).
Um Daten von einem WAN, einem remoten oder separaten Rechenzentrum oder einem anderen geografischen Standort zu erfassen, verwenden Sie Remote-Collectors.
- Remote-Collectors werden durch ein geroutetes Netzwerk unterstützt, jedoch nicht durch NAT.
- Der Hostname eines Clusterknotens darf keinen Unterstrich enthalten.

Best Practices für vRealize Operations Manager -Clusterknoten

Wenn Sie die Cluster-Knoten erstellen, aus denen der vRealize Operations Manager besteht, verbessern Best Practices die Leistung und Zuverlässigkeit im vRealize Operations Manager.

Best Practices

- Stellen Sie vRealize Operations Manager Analyse-Clusterknoten im selben vSphere Cluster in einem einzigen Datacenter bereit und fügen Sie einem Cluster nacheinander nur jeweils einen Knoten hinzu, damit Zeit für die Fertigstellung des Clusters ist, bevor ein weiterer Knoten hinzugefügt wird.
- Wenn Sie Analyse-Clusterknoten in einem höher konsolidierten vSphere-Cluster bereitstellen, müssen Sie für optimale Leistung unter Umständen Ressourcen reservieren.

Bestimmen Sie, ob sich das Verhältnis zwischen virtueller und physischer CPU auf die Leistung auswirkt, indem Sie die CPU-Bereitschaftszeit und Co-Stops prüfen.

- Stellen Sie Analyse-Clusterknoten auf demselben Speicher-Tier-Typ bereit.
- Um die Anforderungen an die Größe und Leistung des Analyse-Clusterknotens weiterhin zu erfüllen, wenden Sie DRS-Antiaffinitätsregeln an, damit sich die Knoten auf unterschiedlichen Datenspeichern befinden.
- Um eine unbeabsichtigte Migration der Knoten zu verhindern, legen Sie Speicher-DRS auf manuell fest.
- Um eine ausgeglichene Leistung der Analyse-Clusterknoten zu gewährleisten, verwenden Sie ESXi-Hosts mit identischen Prozessorfrequenzen. Unterschiedliche Frequenzen und eine abweichende Anzahl physischer Kerne können sich auf die Leistung des Analyse-Clusters auswirken.
- Um einen Leistungsrückgang zu vermeiden, benötigen vRealize Operations Manager-Analyse-Clusterknoten garantierte Ressourcen, wenn sie auf Hochtouren laufen. Die vRealize Operations Manager Knowledgebase enthält Tabellen zur Größenskalkulation, die Ressourcen basierend auf der Anzahl der zu überwachenden Objekte und Metriken, der Verwendung von HA und so weiter berechnen. Bei der Größendefinition ist es besser, mehr Ressourcen als zu wenige zuzuweisen.

Weitere Informationen hierzu finden Sie im [Knowledgebase-Artikel 2093783](#).

- Da Knoten ihre Rollen ändern können, vermeiden Sie Maschinennamen wie Master, Daten, Replikat und so weiter. Beispiele für geänderte Rollen sind die Umwandlung eines Datenknotens in ein Replikat für HA oder die Übernahme der Master-Knotenrolle durch ein Replikat.

- Ab vRealize Operations Manager 6.3 ist die NUMA-Platzierung nicht mehr vorhanden. Vorgehensweisen in Bezug auf die NUMA-Einstellungen der OVA-Datei sind folgende:

Tabelle 1-2. NUMA-Einstellung

Aktion	Beschreibung
Status des vRealize Operations Manager-Clusters auf offline setzen	<ol style="list-style-type: none"> 1 Fahren Sie den vRealize Operations Manager-Cluster herunter. 2 Klicken Sie mit der rechten Maustaste auf den Cluster, und klicken Sie auf Einstellungen bearbeiten > Optionen > Erweitert Allgemein. 3 Klicken Sie auf Konfigurationsparameter. Wiederholen Sie im vSphere Client diese Schritte für jede einzelne VM.
NUMA-Einstellung entfernen	<ol style="list-style-type: none"> 1 Entfernen Sie die Einstellung <code>numa.vcpu.preferHT</code> aus „Konfigurationsparameter“, und klicken Sie auf OK. 2 Klicken Sie auf OK. 3 Wiederholen Sie diese Schritte für alle VMs im vRealize Operations-Cluster. 4 Schalten Sie den Cluster ein.

HINWEIS Um die Verfügbarkeit ausreichender Ressourcen und eine beständige Produktperformance sicherzustellen, überwachen Sie die Performance von vRealize Operations. Überprüfen Sie dazu die Zeiten für CPU-Auslastung, CPU-Bereitschaft und CPU-Konflikt von vRealize Operations.

Verwenden von IPv6 mit vRealize Operations Manager

vRealize Operations Manager unterstützt die Internetprotokoll-Version 6 (IPv6), die Konvention für Netzwerkadressen, die auf lange Sicht IPv4 ersetzen wird. Die Verwendung von IPv6 mit vRealize Operations Manager macht die Einhaltung bestimmter Beschränkungen erforderlich.

Verwenden von IPv6

- Sämtliche vRealize Operations Manager-Cluster-Knoten, einschließlich Remote-Collectors, müssen IPv6-Adressen haben. Nutzen Sie IPv6 und IPv4 nicht gleichzeitig.
- Alle vRealize Operations Manager-Cluster-Knoten, einschließlich Remote-Collectors, müssen auf vApp oder Linux basieren. vRealize Operations Manager für Windows unterstützt IPv6 nicht.
- Verwenden Sie nur globale IPv6-Adressen. Link-lokale Adressen werden nicht unterstützt.
- Wenn einer der Knoten DHCP verwendet, muss Ihr DHCP-Server so konfiguriert sein, dass er IPv6 unterstützt.
- DHCP wird nur auf Datenknoten und Remote-Collectors unterstützt. Masterknoten und Replikatknoten erfordern immer noch statische Adressen. Dies gilt auch bei IPv4.
- Ihr DNS-Server muss so konfiguriert sein, dass er IPv6 unterstützt.
- Wenn Sie dem Knoten Cluster hinzufügen, denken Sie daran, die IPv6-Adresse des Masterknotens einzugeben.
- Wenn Sie eine VMware vCenter[®]-Instanz innerhalb von vRealize Operations Manager registrieren, setzen Sie eckige Klammern um die IPv6-Adresse Ihres VMware vCenter[®]-Serversystems, wenn vCenter ebenfalls IPv6 verwendet.

Beispiel: [2015:0db8:85a3:0042:1000:8a2e:0360:7334]

Beachten Sie: Auch wenn vRealize Operations Manager IPv6 verwendet, hat der vCenter-Server möglicherweise dennoch eine IPv4-Adresse. In diesem Fall benötigt vRealize Operations Manager keine eckigen Klammern.

- Sie können einen Endpoint Operations Management-Agenten nicht in einer Umgebung registrieren, die sowohl IPv4 als auch IPv6 unterstützt. Sollten Sie das versuchen, erscheint der folgende Fehler:

Verbindung fehlgeschlagen. Server heruntergefahren (oder falsche/r IP-Adresse/Port verwendet). Warten Sie 10 Sekunden, bevor Sie es erneut versuchen.

Größenbestimmung des vRealize Operations Manager -Clusters

Die für vRealize Operations Manager erforderlichen Ressourcen hängen von der Größe der Umgebung ab, die Sie überwachen und analysieren möchten, der Anzahl der zu erfassenden Metriken sowie der erforderlichen Speicherdauer der Daten.

Es ist schwierig, die CPU-, Speicher- und Festplattenanforderungen, die den Anforderungen einer bestimmten Umgebung gerecht werden, grob vorzuberechnen. Es gibt viele Variablen, beispielsweise die Anzahl und die Art der erfassten Objekte. Dazu gehören auch die Anzahl und die Art der installierten Adapter, das Vorhandensein von HA, die Dauer der Datenspeicherung und die Menge der jeweiligen interessierenden Daten, wie z. B. Symptome, Änderungen usw.

VMware geht davon aus, dass sich die Sizing-Informationen des vRealize Operations Manager weiter entwickeln, und unterhält Knowledge-Base-Artikel, damit Sizing-Berechnungen an die Nutzungsdaten und Versionsänderung des vRealize Operations Manager angepasst werden können.

[Knowledgebase-Artikel 2093783](#)

Die Knowledgebase-Artikel enthalten Gesamtmaximalwerte sowie Tabellenkalkulationsrechner, in die Sie die Anzahl der zu überwachenden Objekte und Metriken eingeben. Um Zahlen zu erhalten, verwenden einige Benutzer den folgenden allgemeinen Ansatz, den vRealize Operations Manager selbst verwendet.

- 1 Lesen Sie in diesem Handbuch nach, wie ein vRealize Operations Manager-Knoten bereitgestellt und konfiguriert wird.
- 2 Stellen Sie einen temporären vRealize Operations Manager-Knoten bereit.
- 3 Konfigurieren Sie einen oder mehrere Adapter und lassen Sie den temporären Knoten die gewünschten Daten über Nacht erfassen.
- 4 Greifen Sie auf dem temporären Knoten auf die Seite „Cluster-Verwaltung“ zu.
- 5 Verwenden Sie die Liste „Adapterinstanzen“ im unteren Bereich der Anzeige als Referenz und geben Sie die jeweilige Gesamtzahl der Objekte und Metriken der verschiedenen Adaptertypen in die geeignete Größenbestimmungstabelle des [Knowledgebase-Artikels 2093783](#) ein.
- 6 Stellen Sie den vRealize Operations Manager-Cluster auf Basis der Größenempfehlung der Tabelle bereit. Durch Hinzufügen von Ressourcen und Datenknoten zum temporären Knoten oder einen erneuten Versuch können Sie den Cluster aufbauen.

Wenn Sie über eine große Anzahl von Adaptern verfügen, müssen Sie möglicherweise den Vorgang auf dem temporären Knoten zurücksetzen und wiederholen, bis Sie alle benötigten Summen haben. Der temporäre Knoten wird nicht über genug Kapazität verfügen, um gleichzeitig alle Verbindungen eines Großunternehmens zu betreiben.

Ein weiterer Ansatz für die Größenbestimmung bietet die Selbstüberwachung. Stellen Sie den Cluster basierend auf Ihrer Schätzung bereit, erstellen Sie jedoch eine Warnung für die Fälle, wenn die Kapazität unter einen Schwellenwert fällt, der ausreichend Zeit zum Hinzufügen von Knoten oder einem Laufwerk zum Cluster erlaubt. Sie haben auch die Möglichkeit, eine E-Mail-Benachrichtigung für den Fall zu erstellen, dass die Schwellenwerte überschritten werden.

Angepasste vRealize Operations Manager -Zertifikate

Standardmäßig enthält vRealize Operations Manager eigene Authentifizierungszertifikate. Die Standardzertifikate veranlassen den Browser dazu, eine Warnung anzuzeigen, wenn Sie sich mit der vRealize Operations Manager-Benutzeroberfläche verbinden.

Die Sicherheitsrichtlinien für Ihre Umgebung erfordern möglicherweise, dass Sie ein anderes Zertifikat verwenden, oder Sie ziehen es vielleicht vor, die Warnmeldungen zu vermeiden, die von den Standardzertifikaten verursacht werden. In beiden Fällen unterstützt vRealize Operations Manager das Verwenden Ihres eigenen angepassten Zertifikats. Sie können Ihr angepasstes Zertifikat während der Erstkonfiguration des Masterknotens oder später hochladen.

Anforderungen für angepasste vRealize Operations Manager -Zertifikate

Ein mit vRealize Operations Manager verwendetes Zertifikat muss bestimmte Anforderungen erfüllen. Die Verwendung eines benutzerdefinierten Zertifikats ist optional und wirkt sich nicht auf die Funktionen von vRealize Operations Manager aus.

Anforderungen für angepasste Zertifikate

Angepasste vRealize Operations Manager-Zertifikate müssen die folgenden Anforderungen erfüllen.

- Die Zertifikatsdatei muss das Zertifikat des (untergeordneten) Terminalservers, einen privaten Schlüssel und alle herausgebenden Zertifikate enthalten, wenn das Zertifikat von einer Kette von anderen Zertifikaten signiert ist.
- In der Datei muss das untergeordnete Zertifikat an erster Stelle in der Reihenfolge der Zertifikate stehen. Abgesehen von dem untergeordneten Zertifikat spielt die Reihenfolge keine Rolle.
- In der Datei müssen alle Zertifikate und der private Schlüssel dem PEM-Format folgen. vRealize Operations Manager unterstützt keine Zertifikate in den Formaten PFX, PKCS12, PKCS7 oder anderen Formaten.
- In der Datei müssen alle Zertifikate und der private Schlüssel PEM-codiert sein. vRealize Operations Manager unterstützt keine DER-codierten Zertifikate oder privaten Schlüssel.

Die PEM-Codierung ist Base-64 ASCII und enthält lesbare Marker für ANFANG und ENDE. Darüber hinaus entspricht die Dateierweiterung möglicherweise nicht der Codierung. Bei PEM oder DER wird beispielsweise unter Umständen eine allgemeine .cer-Erweiterung verwendet. Untersuchen Sie zur Überprüfung der verwendeten Zeichenkodierung die entsprechende Zertifikatsdatei in einem Texteditor.

- Die Dateierweiterung muss .pem lauten.
- Der private Schlüssel muss vom RSA- oder DSA-Algorithmus generiert werden.
- Der private Schlüssel darf nicht mit einer Passphrase verschlüsselt sein, wenn Sie den Masterknoten-Konfigurationsassistenten oder die Verwaltungsschnittstelle verwenden, um das Zertifikat hochzuladen.
- Die REST-API in dieser vRealize Operations Manager-Version unterstützt private Schlüssel, die mit einer Passphrase verschlüsselt sind. Wenden Sie sich an den Technischen Support von VMware, um weitere Informationen zu erhalten.
- Der vRealize Operations Manager-Webserver hat auf allen Knoten dieselbe Zertifikatsdatei, daher muss sie für alle Knoten gültig sein. Eine der Möglichkeiten, um das Zertifikat für mehrere Adressen gültig zu machen, besteht darin, mehrere alternative Antragstellernamen (Subject Alternative Names, SAN) zu verwenden.

- SHA1-Zertifikate führen zu Problemen mit der Browserkompatibilität. Stellen Sie daher sicher, dass alle erstellten und auf den vRealize Operations Manager hochgeladenen Zertifikate mittels SHA2 oder höher signiert sind.
- vRealize Operations Manager Unterstützt angepasste Sicherheitszertifikate mit einer Schlüssellänge von bis zu 8192 Bits. Falls Sie versuchen, ein Sicherheitszertifikat hochzuladen, das mit einem Schlüssel länger als 8192 Bits generiert worden ist, wird eine Fehlermeldung angezeigt.

Beispielinhalte für angepasste vRealize Operations Manager -Zertifikate

Zur Behebung von Fehlern können Sie die Datei eines angepassten Zertifikats in einem Texteditor öffnen und ihren Inhalt überprüfen.

Zertifikatsdateien im PEM-Format

Eine typische Zertifikatsdatei im PEM-Format ähnelt dem folgenden Beispiel.

```
-----BEGIN CERTIFICATE-----
MIIF1DCCBLYgAwIBAgIKFYXYUwAAAAAAGTANBgkqhkiG9w0BAQ0FADBhMRMwEQYK
CZImiZPyLGBGRYDY29tMRUwEwYKCZImiZPyLGBGRYFdm13Y3MxGDAWBgoJkiaJ
<snip>
vKStQJNr7z2+pTy92M6FgJz3y+daL+9ddbaMnp9fVXjHBoDLGGaL0vyD+KJ8+xba
aGJfGf9ELXM=
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQE415ffX694riIIRmdRLJwL6sOWa+Wf70HRoLtx21kZzbXbUQN
mQhTRidJ3Ro2gRbj/btSsI+OMUzotz5VRT/yeyoTC5l2uJEapld45RroUDHQwWJ
<snip>
DAN9hQus3832xMkAuVP/jt76dHDYyviyIYbmzxMa1X7LZy1MCQVg4hCH0vLsHtLh
M1rOAsz62Eht/iB61AsVCCiN3gLRX7MKsYdxZcRVruGXSih33ynA
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDnTCCAowgAwIBAgIQY+j29InmdYNCs2cK1H4kPzANBgkqhkiG9w0BAQ0FADBh
MRMwEQYKCZImiZPyLGBGRYDY29tMRUwEwYKCZImiZPyLGBGRYFdm13Y3MxGDAW
<snip>
ukzUuqX7wEhc+QgJWgl41mWZBZ09gfsA9XuXBL0k17IpVHpEgwwrjQz8X68m4I99
dD5Pf1f/nLRJvR9jwXl62yk=
-----END CERTIFICATE-----
```

Private Schlüssel

Private Schlüssel können in verschiedenen Formaten erscheinen, sind aber mit deutlichen Markern für ANFANG und ENDE umschlossen.

Gültige PEM-Abschnitte beginnen mit einem der folgenden Marker.

```
-----BEGIN RSA PRIVATE KEY-----
-----BEGIN PRIVATE KEY-----
```

Verschlüsselte private Schlüssel beginnen mit dem folgenden Marker.

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
```

Bag-Attribute

Zertifikatstools von Microsoft fügen Zertifikatsdateien manchmal Abschnitte mit Bag-Attributen hinzu. vRealize Operations Manager ignoriert Inhalte außerhalb von Markern für ANFANG und ENDE problemlos, einschließlich Abschnitte mit Bag-Attributen.

Bag Attributes

Microsoft Local Key set: <No Values>

localKeyID: 01 00 00 00

Microsoft CSP Name: Microsoft RSA SChannel Cryptographic Provider
friendlyName: le-WebServer-8dea65d4-c331-40f4-aa0b-205c3c323f62

Key Attributes

X509v3 Key Usage: 10

-----BEGIN PRIVATE KEY-----

```
MIICdwIBADANBgkqhkiG9w0BAQEFAASCAmEwgGJdAgEAAoGBAKHqyfc+qcQK4yxJ
om3PuB8dYZm34Qlt81GAAnBPYe3B4Q/0ba6PV8GtWG2svIpcI/eflwGHgTU3zJxR
gkKh7I3K5tGESn81ipyKtkPbYebh+aBMqPKrNNUEKlr0M9sa3WSc0o3350tCc1ew
5ZkNYZ4BRUVYwM0HogeGh0thRn2fAgMBAECgYABhPmGN3FSZKPDG6HJLARvTLBH
KAGVnBGHd0MOMABghFBnBKXa8LwD1dgGBng1oOakEXTftkIjdB+uwkU5P4aRr07
vGujUtRyRCU/4fjLBDuxQL/KpQfruAQaof9uUwh5W9fEeW3g26fzVL8AFZnbXS0
7Z0AL1H3LncLd5rPQJBAAnnI7vFu06bFxFV+kq6Z0JFMx7x3K4VGxgg+PfFEBEPS
UJ2LuDH5/Rc63BaxFzM/q3B3Jhehvgw61mMyxU7QSSUCQC+VDuW3XEWJjSiU6KD
gEGpCyJ5SBePbLSukljPgidKkDNlKlgbWVytCVkTAmuoAz33kMWfqiInCqQbUgVV
UnpzAkB7d0CP00deSsy8kMdTmKXLKf4qSF0x55epYK/5MZhBYuA1ENrR6mmjw8ke
TDNc6IGm9sVvrFBz2n9kKYpWThrJAkEAK5R69DtW0cbkLy5MqEzOHQauP36gDi1L
WMXPvUfzSYTQ5aM2rrY2/1FtSSkqUwFYh9sw8eDbqVpIV4rc6dDfcwJBALiiDPT0
tz86wySJNe0iUkQm36iXVF8AckPKT9TrbC3Ho7nC80zL7gEl1ETa4Zc86Z3wpcGF
BHhEDMHaihyuVgI=
```

-----END PRIVATE KEY-----

Bag Attributes

localKeyID: 01 00 00 00

1.3.6.1.4.1.311.17.3.92: 00 04 00 00

1.3.6.1.4.1.311.17.3.20: 7F 95 38 07 CB 0C 99 DD 41 23 26 15 8B E8
D8 4B 0A C8 7D 93

friendlyName: cos-oc-vcops

1.3.6.1.4.1.311.17.3.71: 43 00 4F 00 53 00 2D 00 4F 00 43 00 2D 00
56 00 43 00 4D 00 35 00 37 00 31 00 2E 00 76 00 6D 00 77 00 61 00
72 00 65 00 2E 00 63 00 6F 00 6D 00 00 00

1.3.6.1.4.1.311.17.3.87: 00 00 00 00 00 00 00 00 02 00 00 00 20 00
00 00 02 00 00 00 6C 00 64 00 61 00 70 00 3A 00 00 00 7B 00 41 00
45 00 35 00 44 00 44 00 33 00 44 00 30 00 2D 00 36 00 45 00 37 00
30 00 2D 00 34 00 42 00 44 00 42 00 2D 00 39 00 43 00 34 00 31 00
2D 00 31 00 43 00 34 00 41 00 38 00 44 00 43 00 42 00 30 00 38 00
42 00 46 00 7D 00 00 00 70 00 61 00 2D 00 61 00 64 00 63 00 33 00
2E 00 76 00 6D 00 77 00 61 00 72 00 65 00 2E 00 63 00 6F 00 6D 00
5C 00 56 00 4D 00 77 00 61 00 72 00 65 00 20 00 43 00 41 00 00 00
31 00 32 00 33 00 33 00 30 00 00 00

subject=/CN=cos-oc-vcops.eng.vmware.com

issuer=/DC=com/DC=vmware/CN=VMware CA

-----BEGIN CERTIFICATE-----

```
MIIFWTCBEGgAwIBAgIKSJGT5gACAAAwKjANBgkqhkiG9w0BAQUFAADBMRMwEQYK
CZImiZPyLGBGRYDY29tMRYwFAYKCCImiZPyLGBGRYDm13YXJlMRlWIAEYDVQQD
EwltWtXdhcmUgQ0EwHhcnMTQwMjA1MTg1OTM2WhcnMTYwMjA1MTg1OTM2WjAmMSQw
```

Überprüfen eines angepassten vRealize Operations Manager -Zertifikats

Wenn Sie eine angepasste Zertifikatsdatei hochladen, zeigt die Schnittstelle von vRealize Operations Manager Übersichtsinformationen über alle Zertifikate in der Datei an.

Bei einer gültigen angepassten Zertifikatsdatei sollten Sie in der Lage sein, den Aussteller dem Antragsteller zuzuordnen, bis zurück zu einem selbstsignierten Zertifikat, bei dem der Aussteller und der Antragsteller identisch sind.

In dem folgenden Beispiel wurde OU=MBU,O=VMware\, Inc.,CN=vc-ops-slice-32 von OU=MBU,O=VMware\, Inc.,CN=vc-ops-intermediate-32 ausgestellt, das von OU=MBU,O=VMware\, Inc.,CN=vc-ops-cluster-ca_33717ac0-ad81-4a15-ac4e-e1806f0d3f84 ausgestellt wurde, das von sich selbst ausgestellt wurde.

```
Thumbprint: 80:C4:84:B9:11:5B:9F:70:9F:54:99:9E:71:46:69:D3:67:31:2B:9C
Issuer Distinguished Name: OU=MBU,O=VMware\, Inc.,CN=vc-ops-intermediate-32
Subject Distinguished Name: OU=MBU,O=VMware\, Inc.,CN=vc-ops-slice-32
Subject Alternate Name:
PublicKey Algorithm: RSA
Valid From: 2015-05-07T16:25:24.000Z
Valid To: 2020-05-06T16:25:24.000Z
```

```
Thumbprint: 72:FE:95:F2:90:7C:86:24:D9:4E:12:EC:FB:10:38:7A:DA:EC:00:3A
Issuer Distinguished Name: OU=MBU,O=VMware\, Inc.,CN=vc-ops-cluster-ca_33717ac0-ad81-4a15-ac4e-e1806f0d3f84
Subject Distinguished Name: OU=MBU,O=VMware\, Inc.,CN=vc-ops-intermediate-32
Subject Alternate Name: localhost,127.0.0.1
PublicKey Algorithm: RSA
Valid From: 2015-05-07T16:25:19.000Z
Valid To: 2020-05-06T16:25:19.000Z
```

```
Thumbprint: FA:AD:FD:91:AD:E4:F1:00:EC:4A:D4:73:81:DB:B2:D1:20:35:DB:F2
Issuer Distinguished Name: OU=MBU,O=VMware\, Inc.,CN=vc-ops-cluster-ca_33717ac0-ad81-4a15-ac4e-e1806f0d3f84
Subject Distinguished Name: OU=MBU,O=VMware\, Inc.,CN=vc-ops-cluster-ca_33717ac0-ad81-4a15-ac4e-e1806f0d3f84
Subject Alternate Name: localhost,127.0.0.1
PublicKey Algorithm: RSA
Valid From: 2015-05-07T16:24:45.000Z
Valid To: 2020-05-06T16:24:45.000Z
```


Erstellen des vRealize Operations Manager - Master-Knotens

2

Alle vRealize Operations Manager-Installationen erfordern einen Master-Knoten.

Dieses Kapitel behandelt die folgenden Themen:

- „Über den vRealize Operations Manager-Master-Knoten“, auf Seite 21
- „Ausführen des Setup-Assistenten zum Erstellen des Master-Knotens“, auf Seite 21

Über den vRealize Operations Manager -Master-Knoten

Der Master-Knoten ist der erforderliche, erste Knoten in Ihrem vRealize Operations Manager-Cluster

Bei Einzelknoten-Clustern befinden sich die Verwaltung und die Daten auf demselben Master-Knoten. Ein Mehrknoten-Cluster enthält einen Master-Knoten und einen bzw. mehr Datenknoten. Außerdem können Remote-Collector-Knoten vorhanden sein und für High Availability kann auch ein Replikationsknoten eingerichtet werden.

Der Master-Knoten führt die Verwaltung für den Cluster durch und muss online sein, bevor Sie neue Knoten konfigurieren. Außerdem muss der Master-Knoten online sein, bevor andere Knoten online gebracht werden. Wenn Master- und Replikationsknoten zusammen offline geschaltet werden, schalten Sie sie getrennt wieder online. Schalten Sie zuerst den Masterknoten wieder vollständig online und schalten Sie dann den Replikationsknoten online. Beispiel: Wenn der gesamte Cluster aus einem beliebigen Grund offline war, bringen Sie den Master-Knoten zuerst online.



Erstellen des Master-Knotens (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vrops_create_master_node)

Ausführen des Setup-Assistenten zum Erstellen des Master-Knotens

Alle vRealize Operations Manager-Installationen erfordern einen Master-Knoten. Bei einem Einzelknoten-Cluster befinden sich die Verwaltungs- und Datenfunktionen auf demselben Master-Knoten. Ein vRealize Operations Manager-Cluster mit mehreren Knoten enthält einen Master-Knoten und mindestens einen Knoten für die Handhabung zusätzlicher Daten.

Voraussetzungen

- Notieren Sie nach Bereitstellung des Knotens dessen vollqualifizierten Domännennamen (FQDN) bzw. dessen IP-Adresse.
- Wenn Sie vorhaben, ein angepasstes Authentifizierungszertifikat zu verwenden, stellen Sie sicher, dass Ihr Zertifikat die Anforderungen für vRealize Operations Manager erfüllt. Weitere Informationen hierzu finden Sie unter „Angepasste vRealize Operations Manager-Zertifikate“, auf Seite 16.

Vorgehensweise

- 1 Navigieren Sie zum Namen bzw. zur IP-Adresse des Knotens, der als Master-Knoten von vRealize Operations Manager dienen soll.

Der Setup-Assistent wird angezeigt, und Sie müssen sich nicht bei vRealize Operations Manager anmelden.
- 2 Klicken Sie auf **Neue Installation**.
- 3 Klicken Sie auf **Weiter**.
- 4 Geben Sie ein Kennwort für das Admin-Benutzerkonto ein, bestätigen Sie es und klicken Sie auf **Weiter**.

Das Kennwort muss mindestens acht Zeichen lang sein und einen Großbuchstaben, einen Kleinbuchstaben, eine Ziffer und ein Sonderzeichen enthalten.

Der Name des Benutzerkontos lautet standardmäßig „admin“ und kann nicht geändert werden.
- 5 Wählen Sie, ob Sie das mit vRealize Operations Manager mitgelieferte Zertifikat verwenden oder ein eigenes Zertifikat installieren möchten.
 - a Um ein eigenes Zertifikat zu verwenden, klicken Sie auf **Durchsuchen**, navigieren Sie zur Zertifikatsdatei und klicken Sie auf **Öffnen**, um die Datei in das Textfeld „Zertifikatsinformationen“ zu laden.
 - b Überprüfen Sie die erkannten Informationen über Ihr Zertifikat, um zu verifizieren, dass es den Anforderungen an vRealize Operations Manager genügt.
- 6 Klicken Sie auf **Weiter**.
- 7 Geben Sie einen Namen für den Master-Knoten ein.

Beispiel: **Ops-Master**
- 8 Geben Sie die URL oder IP-Adresse für den NTP-Server (Network Time Protocol) ein, mit dem der Cluster synchronisiert werden wird.

Beispiel: **time.nist.gov**
- 9 Klicken Sie auf **Hinzufügen**.

Geben Sie keinen NTP-Server an, wenn Sie möchten, dass vRealize Operations Manager die eigene Synchronisierung steuert, indem alle Knoten mit dem Master-Knoten und dem Replikationsknoten synchronisiert werden.
- 10 Klicken Sie auf **Weiter** und anschließend auf **Beenden**.

Die Verwaltungsschnittstelle wird angezeigt und es dauert einen Moment, bis vRealize Operations Manager den Master-Knoten hinzugefügt hat.

Weiter

Nachdem Sie den Master-Knoten erstellt haben, haben Sie folgende Optionen.

- Erstellen Sie Datenknoten und fügen Sie sie zum nicht gestarteten Cluster hinzu.
- Erstellen Sie Remote Collector-Knoten und fügen Sie sie zum nicht gestarteten Cluster hinzu.
- Klicken Sie auf **vRealize Operations Manager starten**, um den Einzelknoten-Cluster zu starten, und melden Sie sich an, um das Konfigurieren des Produkts abzuschließen.

Je nach Größe des Clusters und der Knoten kann es 10 bis 30 Minuten dauern, bis der Cluster gestartet ist. Während der Cluster gestartet wird, nehmen Sie keine Änderungen an den Clusterknoten vor und führen Sie keine Aktionen auf sie aus.

Horizontales Skalieren von vRealize Operations Manager durch Hinzufügen eines Datenknotens

3

Sie können zusätzliche Knoten bereitstellen und konfigurieren, damit vRealize Operations Manager größere Umgebungen unterstützen kann.

Dieses Kapitel behandelt die folgenden Themen:

- „Über vRealize Operations Manager-Datenknoten“, auf Seite 23
- „Ausführen des Setup-Assistenten zum Hinzufügen eines Datenknotens“, auf Seite 24

Über vRealize Operations Manager -Datenknoten

Datenknoten sind die zusätzlichen Clusterknoten, mit denen Sie vRealize Operations Manager horizontal skalieren können, um größere Umgebungen zu überwachen.

Ein Datenknoten teilt grundsätzlich die Arbeitslast zur Ausführung von vRealize Operations Manager-Analysen. Außerdem kann ein Lösungsadapter installiert sein, um die Erfassung und die Speicherung von Daten aus der Umgebung durchzuführen. Sie müssen einen Master-Knoten eingerichtet haben, bevor Sie Datenknoten hinzufügen können.

Sie können vRealize Operations Manager dynamisch horizontal skalieren, indem Sie Datenknoten hinzufügen, ohne den vRealize Operations Manager-Cluster anzuhalten. Wenn Sie den Cluster um 25 % oder mehr horizontal skalieren, müssen Sie den Cluster neu starten, damit vRealize Operations Manager seine Speichergröße aktualisieren kann. Ein Rückgang der Leistung kann eintreten, bis Sie einen Neustart ausgeführt haben. Ein Wartungsintervall bietet eine gute Gelegenheit, um den vRealize Operations Manager-Cluster neu zu starten.

Außerdem enthalten die Optionen für die Produktadministration eine Option zur Neuverteilung des Clusters. Dies kann ohne Neustart erfolgen. Durch die Neuverteilung wird die vRealize Operations Manager-Arbeitslast über die Clusterknoten verteilt.

HINWEIS Fahren Sie Online-Clusterknoten nicht extern oder mit anderen Mitteln als der vRealize Operations Manager-Oberfläche herunter. Fahren Sie einen Knoten nur extern herunter, nachdem Sie ihn in der vRealize Operations Manager-Oberfläche offline geschaltet haben.



Erstellen eines Datenknotens (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vrops_create_data_node)

Ausführen des Setup-Assistenten zum Hinzufügen eines Datenknotens

In größeren Umgebungen mit vRealize Operations Manager-Clustern mit mehreren Knoten gibt es einen Masterknoten und mindestens einen Datenknoten für die zusätzliche Datenerfassung, Speicherung, Verarbeitung und Analyse.

Voraussetzungen

- Erstellen und konfigurieren Sie den Master-Knoten.
- Merken Sie sich den vollständig qualifizierten Domännennamen (FQDN) oder die IP-Adresse des Master-Knotens.

Vorgehensweise

- 1 Navigieren Sie in einem Webbrowser zum Namen oder zur IP-Adresse des Knotens, der zum Datenknoten wird.

Der Setup-Assistent wird angezeigt, und Sie müssen sich nicht bei vRealize Operations Manager anmelden.

- 2 Klicken Sie auf **Vorhandene Installation erweitern**.
- 3 Klicken Sie auf **Weiter**.
- 4 Geben Sie einen Namen für den Knoten ein (z. B. **Daten-1**).
- 5 Wählen Sie im Dropdown-Menü „Knotentyp“ die Option **Daten** aus.
- 6 Geben Sie den FQDN oder die IP-Adresse des Master-Knotens ein und klicken Sie auf **Validieren**.
- 7 Wählen Sie **Dieses Zertifikat akzeptieren** aus und klicken Sie dann auf **Weiter**.

Suchen Sie bei Bedarf das Zertifikat auf dem Masterknoten und überprüfen Sie den Fingerabdruck.

- 8 Überprüfen Sie den vRealize Operations Manager-Administratorbenutzernamen des Administrators.
- 9 Geben Sie das Administratorkennwort von vRealize Operations Manager ein.

Alternativ können Sie anstelle eines Kennworts eine Passphrase eingeben, die Sie von Ihrem vRealize Operations Manager-Administrator erhalten haben.

- 10 Klicken Sie auf **Weiter** und anschließend auf **Beenden**.

Die Verwaltungsschnittstelle wird angezeigt und das Hinzufügen des Datenknotens durch vRealize Operations Manager nimmt eine gewisse Zeit in Anspruch.

Weiter

Nachdem Sie einen Datenknoten erstellt haben, haben Sie folgende Optionen.

- Neue, nicht gestartete Cluster:
 - Erstellen Sie weitere Datenknoten und fügen Sie sie hinzu.
 - Erstellen Sie Remote Collector-Knoten und fügen Sie sie hinzu.
 - Erstellen Sie einen Hochverfügbarkeits-Masterreplikatknoten.
 - Klicken Sie auf **vRealize Operations Manager starten**, um den Cluster zu starten, und melden Sie sich an, um das Konfigurieren des Produkts abzuschließen.

Je nach Größe des Clusters und der Knoten kann es 10 bis 30 Minuten dauern, bis der Cluster gestartet ist. Während der Cluster gestartet wird, nehmen Sie keine Änderungen an den Clusterknoten vor und führen Sie keine Aktionen auf sie aus.

- Etablierte, laufende Knoten:
 - Erstellen Sie weitere Datenknoten und fügen Sie sie hinzu.
 - Erstellen Sie weitere Remote Collector-Knoten und fügen Sie sie hinzu.
 - Erstellen Sie einen Hochverfügbarkeits-Masterreplikatknoten, der einen Cluster-Neustart erfordert.

Hinzufügen von High Availability zu vRealize Operations Manager

4

Sie können einen vRealize Operations Manager-Clusterknoten speziell einrichten, sodass er als Replikationsknoten für den vRealize Operations Manager-Master-Knoten fungiert.

Dieses Kapitel behandelt die folgenden Themen:

- „Über vRealize Operations Manager High Availability“, auf Seite 27
- „Ausführen des Setup-Assistenten zum Hinzufügen eines Master-Replikationsknotens“, auf Seite 28

Über vRealize Operations Manager High Availability

vRealize Operations Manager unterstützt High Availability (HA). HA erzeugt ein Replikat für den vRealize Operations Manager-Masterknoten und schützt der Analyse-Cluster vor dem Verlust eines Knotens.

Mit HA werden Daten, die auf dem Master-Knoten gespeichert sind, immer zu 100 % auf dem Replikationsknoten gesichert. Um HA zu aktivieren, muss zusätzlich zum Master-Knoten mindestens ein Datenknoten bereitgestellt sein.

- HA ist kein Mechanismus für Disaster Recovery. HA schützt der Analyse-Cluster nur vor dem Verlust eines Knotens und weil nur ein Verlust abgedeckt ist, können Sie die Knoten nicht auf vSphere-Cluster ausweiten, um Knoten zu isolieren oder Ausfallzonen zu erstellen.
- Wenn HA aktiviert ist, kann das Replikat alle Funktionen übernehmen, die der Master bereitstellt, sollte der Master aus irgendeinem Grund ausfallen. Wenn der Master ausfällt, findet das Failover auf das Replikat automatisch statt und vRealize Operations Manager fällt nur drei Minuten lang aus, bevor der Betrieb wieder aufgenommen und die Datenerfassung neu gestartet wird.

Wenn ein Problem mit dem Datenknoten zum Failover führt, wird der Replikatknoten zum Masterknoten und der Cluster läuft im heruntergestuften Modus. Um den heruntergestuften Modus zu verlassen, führen Sie einen der folgenden Schritte aus.

- Kehren Sie zum HA-Modus zurück, indem Sie das Problem mit dem Masterknoten beheben. Wenn ein Masterknoten ein HA-aktiviertes Cluster verlässt, verbindet sich der Masterknoten nicht ohne manuellen Eingriff mit dem Cluster. Starten Sie daher den vRealize Operations-Analyseprozess am ausgefallenen Knoten, um dessen Rolle auf Replikat zu ändern und ihn wieder mit dem Cluster zu verbinden.
- Kehren Sie zum HA-Modus zurück, indem Sie einen Datenknoten in einen neuen Replikatknoten konvertieren und dann den alten, ausgefallenen Masterknoten entfernen. Entfernte Masterknoten können nicht repariert und erneut zu vRealize Operations Manager hinzugefügt werden.
- Wechseln Sie zum Nicht-HA-Betrieb, indem Sie HA deaktivieren und dann den alten, ausgefallenen Masterknoten entfernen. Entfernte Masterknoten können nicht repariert und erneut zu vRealize Operations Manager hinzugefügt werden.

- Nachdem ein HA-Replikatknoten übernommen hat und zum neuen Masterknoten wird, können Sie in der Verwaltungsschnittstelle den vorherigen Offline-Masterknoten nicht aus dem Cluster entfernen. Außerdem wird der vorherige Knoten weiterhin als ein Masterknoten aufgeführt. Um die Anzeige zu aktualisieren und das Entfernen des Knotens zu aktivieren, aktualisieren Sie den Browser.
- Wenn HA aktiviert ist, kann der Cluster den Verlust eines Datenknotens ohne Datenverlust bewältigen. Doch HA schützt immer nur vor dem Verlust eines Knotens beliebiger Art. Das heißt, der gleichzeitige Verlust von Daten- und Master-/Replikatknoten oder von zwei oder mehr Datenknoten ist nicht abgedeckt. Stattdessen bietet vRealize Operations Manager-HA zusätzlichen Datenschutz auf Anwendungsebene, um die Verfügbarkeit auf Anwendungsebene zu gewährleisten.
- Wenn HA aktiviert ist, werden vRealize Operations Manager-Kapazität und -Verarbeitung halbiert, weil HA eine redundante Kopie der Daten im Cluster sowie die Replikatsicherung des Masterknoten erstellt. Bedenken Sie die mögliche Verwendung von HA, wenn Sie die Anzahl und Größe Ihrer vRealize Operations Manager-Cluster-Knoten planen. Weitere Informationen hierzu finden Sie unter „Größenbestimmung des vRealize Operations Manager-Clusters“, auf Seite 15.
- Wenn HA aktiviert ist, stellen Sie Analyse-Cluster-Knoten auf separaten Hosts bereit, um Redundanz und Isolation zu erreichen. Eine Option ist die Verwendung von Antiaffinitätsregeln, die Knoten auf separaten Hosts im vSphere-Cluster halten.

Wenn Sie die Knoten nicht separat halten können, sollten Sie HA aktivieren. Ein Host-Fehler würde zum Verlust mehrerer Knoten führen, was nicht abgedeckt ist, und der gesamte vRealize Operations Manager würde nicht verfügbar werden.

Das gilt auch für das Gegenteil. Ohne HA können Sie Knoten auf demselben Host halten und es macht keinen Unterschied. Ohne HA würde durch den Verlust eines Knotens der gesamte vRealize Operations Manager nicht verfügbar werden.

- Wenn Sie den Datenknoten ausschalten und die Netzwerkeinstellungen der VM ändern, wirkt sich dies auf die IP-Adresse des Datenknotens aus. Danach kann nicht mehr auf den HA-Knoten zugegriffen werden und alle Knoten haben den Status „Warten auf Analyse.“ Stellen Sie sicher, dass eine statische IP-Adresse verwendet wurde.
- Wenn Sie einen Knoten entfernen, bei dem ein oder mehrere vCenter-Adapter so konfiguriert sind, dass sie von einem HA-aktivierten Cluster Daten erfassen, stellen ein oder mehrere vCenter-Adapter, die diesem Knoten zugeordnet sind, ihren Dienst zur Datenerfassung ein. Bevor Sie den Knoten entfernen sollten Sie die Adapterkonfiguration so ändern, dass sie auf einen anderen Knoten zugreifen.
- Die Verwaltungs-Benutzerschnittstelle zeigt den Ressourcen-Cache-Zähler, der nur für aktive Objekte erstellt wird, aber der Bestands-Explorer zeigt alle Objekte an. Wenn Sie von einem HA-aktiviertem Cluster einen Knoten entfernen, bei dem die vCenter-Adapter Daten erfassen können, und dann die Last der einzelnen Knoten neu verteilen, zeigt der Bestands-Explorer demzufolge eine andere Anzahl an Objekten als die Verwaltungs-Benutzerschnittstelle.



Erstellen eines Replikatknotens für High Availability (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vrops_create_replica_node_ha)

Ausführen des Setup-Assistenten zum Hinzufügen eines Master-Replikationsknotens

Sie können einen vRealize Operations Manager-Datenknoten in ein Replikat des Master-Knotens konvertieren. Dies fügt High Availability (HA) für vRealize Operations Manager hinzu.

HINWEIS Wenn der Cluster läuft, wird der Cluster durch Aktivieren von HA neu gestartet.

Wenn Sie einen Datenknoten konvertieren, der bereits für die Datenerfassung und -analyse verwendet wird, erfolgt ein Failover der Adapter und Datenverbindungen, die dieser Datenknoten bereitgestellt hat, auf andere Datenknoten.

Sie können HA während der Installation oder der Ausführung von vRealize Operations Manager zum vRealize Operations Manager-Cluster hinzufügen. Das Hinzufügen von HA während der Installation ist weniger störend, da der Cluster noch nicht gestartet wurde.

Voraussetzungen

- Erstellen und konfigurieren Sie den Master-Knoten.
- Erstellen und konfigurieren Sie einen Datenknoten mit einer statischen IP-Adresse.
- Merken Sie sich den vollständig qualifizierten Domännennamen (FQDN) oder die IP-Adresse des Master-Knotens.

Vorgehensweise

- 1 Navigieren Sie in einem Webbrowser zur Verwaltungsschnittstelle des Master-Knotens.
`https://Name_oder_IP-Adresse_des_Master-Knotens/admin`
- 2 Geben Sie den vRealize Operations Manager-Administratorbenutzernamen **admin** ein.
- 3 Geben Sie das vRealize Operations Manager-Administratorkennwort ein und klicken Sie auf **Anmelden**.
- 4 Klicken Sie unter „High Availability“ auf **Aktivieren**.
- 5 Wählen Sie einen Datenknoten aus, der als Replikat für den Master-Knoten dienen soll.
- 6 Wählen Sie die Option **Hochverfügbarkeit für diesen Cluster aktivieren** und klicken Sie auf **OK**.
Wenn der Cluster online war, wird der Fortschritt auf der Verwaltungsschnittstelle gezeigt, wenn vRealize Operations Manager den Cluster für HA konfiguriert, synchronisiert und neu verteilt.
- 7 Wenn der Master-Knoten und der Replikat-Knoten offline gehen und der Master aus irgendeinem Grund offline bleibt, wenn der Replikat-Knoten wieder online geht, übernimmt der Replikat-Knoten nicht die Master-Rolle. Nehmen Sie den gesamten Cluster einschließlich Datenknoten offline, und melden Sie sich als „root“ an der Befehlszeilenkonsole des Replikat-Knotens an.
- 8 Öffnen Sie `$ALIVE_BASE/persistence/persistence.properties` in einem Texteditor.
- 9 Suchen Sie die folgenden Eigenschaften, und legen Sie sie fest:
`db.role=MASTER`
`db.driver=/data/vcops/xdb/vcops.bootstrap`
- 10 Speichern und schließen Sie `persistence.properties`.
- 11 Öffnen Sie die Administrationsschnittstelle, bringen Sie den Replikat-Knoten online, stellen Sie sicher, dass der Replikat-Knoten zum Master-Knoten wird, und bringen Sie die übrigen Cluster-Knoten online.

Weiter

Nachdem Sie einen Masterreplikatknoten erstellt haben, haben Sie folgende Optionen.

- Neue, nicht gestartete Cluster:
 - Erstellen Sie Datenknoten und fügen Sie sie hinzu.
 - Erstellen Sie Remote Collector-Knoten und fügen Sie sie hinzu.
 - Klicken Sie auf **vRealize Operations Manager starten**, um den Cluster zu starten, und melden Sie sich an, um das Konfigurieren des Produkts abzuschließen.

Je nach Größe des Clusters und der Knoten kann es 10 bis 30 Minuten dauern, bis der Cluster gestartet ist. Während der Cluster gestartet wird, nehmen Sie keine Änderungen an den Clusterknoten vor und führen Sie keine Aktionen auf sie aus.

- Etablierte, laufende Knoten:
 - Erstellen Sie Datenknoten und fügen Sie sie hinzu.
 - Erstellen Sie weitere Remote Collector-Knoten und fügen Sie sie hinzu.

Erfassen weiterer Daten durch Hinzufügen eines vRealize Operations Manager - Remote-Collector-Knotens

5

Die Bereitstellung und Konfiguration eines Remote-Collector-Knotens erfolgt, damit vRealize Operations Manager seinem Bestand an zu überwachenden Objekten weitere hinzufügen kann, ohne die Verarbeitungslast für vRealize Operations Manager-Analysefunktionen zu erhöhen.

Dieses Kapitel behandelt die folgenden Themen:

- [„Über vRealize Operations Manager-Remote-Collector-Knoten“](#), auf Seite 31
- [„Ausführen des Setup-Assistenten zum Erstellen eines Remote Collector-Knotens“](#), auf Seite 31

Über vRealize Operations Manager -Remote-Collector-Knoten

Ein Remote-Collector-Knoten ist ein zusätzlicher Clusterknoten, der vRealize Operations Manager ermöglicht, mehr Objekte in den Bestand zur Überwachung aufzunehmen. Anders als Datenknoten enthalten Remote-Collector-Knoten nur die Collector-Rolle von vRealize Operations Manager, und keine Datenspeicherungs- oder Analysefunktionen.

Ein Remote-Collector-Knoten wird normalerweise bereitgestellt, um über Firewalls zu navigieren, eine Schnittstelle mit einer Remote-Datenquelle herzustellen, Bandbreitenbedarf zwischen Rechenzentren zu reduzieren oder die Arbeitslast für den vRealize Operations Manager-Analyse-Cluster zu reduzieren.

Remote Collectors puffern keine Daten, wenn das Netzwerk ein Problem hat. Wenn die Verbindung zwischen dem Remote Collector und dem Analyse-Cluster unterbrochen wird, speichert der Remote Collector keine Datenpunkte, die während dieser Zeit auftreten. Im Gegenzug und nachdem die Verbindung wieder hergestellt wurde, nimmt vRealize Operations Manager rückwirkend keine verwandten Ereignisse von dieser Zeit in Überwachungen oder Analysen auf.

Sie müssen mindestens über einen Master-Knoten verfügen, bevor Sie Remote-Collector-Knoten hinzufügen.

Ausführen des Setup-Assistenten zum Erstellen eines Remote Collector-Knotens

In verteilten vRealize Operations Manager-Umgebungen erhöhen Remote Collector-Knoten den Objektbestand, der überwacht werden kann, ohne die Auslastung für vRealize Operations Manager im Hinblick auf die Datenspeicherung, -verarbeitung oder -analyse zu erhöhen.

Voraussetzungen

- Erstellen und konfigurieren Sie den Master-Knoten.
- Merken Sie sich den vollständig qualifizierten Domännennamen (FQDN) oder die IP-Adresse des Master-Knotens.

Vorgehensweise

- 1 Navigieren Sie in einem Webbrowser zum Namen oder zur IP-Adresse der bereitgestellten OVF-Instanz, die zum Remote Collector-Knoten wird.
Der Setup-Assistent wird angezeigt, und Sie müssen sich nicht bei vRealize Operations Manager anmelden.
- 2 Klicken Sie auf **Vorhandene Installation erweitern**.
- 3 Klicken Sie auf **Weiter**.
- 4 Geben Sie einen Namen für den Knoten ein, z. B. **Remote-1**.
- 5 Wählen Sie im Dropdown-Menü **Knotentyp** die Option **Remote Collector** aus.
- 6 Geben Sie den FQDN oder die IP-Adresse des Master-Knotens ein und klicken Sie auf **Validieren**.
- 7 Wählen Sie **Dieses Zertifikat akzeptieren** aus und klicken Sie dann auf **Weiter**.
Suchen Sie bei Bedarf das Zertifikat auf dem Masterknoten und überprüfen Sie den Fingerabdruck.
- 8 Verifizieren Sie den vRealize Operations Manager Administratorbenutzernamen **admin**.
- 9 Geben Sie das Administratorkennwort von vRealize Operations Manager ein.
Alternativ können Sie anstelle eines Kennworts eine Passphrase eingeben, die Sie vom vRealize Operations Manager-Administrator erhalten haben.
- 10 Klicken Sie auf **Weiter** und anschließend auf **Beenden**.
Die Verwaltungsschnittstelle wird angezeigt und es dauert einige Minuten, bis vRealize Operations Manager den Remote Collector-Knoten hinzugefügt hat.

Weiter

Nachdem Sie einen Remote Collector-Knoten erstellt haben, haben Sie folgende Optionen.

- Neue, nicht gestartete Cluster:
 - Erstellen Sie Datenknoten und fügen Sie sie hinzu.
 - Erstellen Sie Remote Collector-Knoten und fügen Sie sie hinzu.
 - Erstellen Sie einen Hochverfügbarkeits-Masterreplikatknoten.
 - Klicken Sie auf **vRealize Operations Manager starten**, um den Cluster zu starten, und melden Sie sich an, um das Konfigurieren des Produkts abzuschließen.
Je nach Größe des Clusters und der Knoten kann es 10 bis 30 Minuten dauern, bis der Cluster gestartet ist. Während der Cluster gestartet wird, nehmen Sie keine Änderungen an den Clusterknoten vor und führen Sie keine Aktionen auf sie aus.
- Etablierte, laufende Knoten:
 - Erstellen Sie Datenknoten und fügen Sie sie hinzu.
 - Erstellen Sie Remote Collector-Knoten und fügen Sie sie hinzu.
 - Erstellen Sie einen Hochverfügbarkeits-Masterreplikatknoten, der einen Cluster-Neustart erfordert.

Fortfahren mit einer vRealize Operations Manager - Neuinstallation

6

Nachdem Sie die vRealize Operations Manager-Knoten bereitgestellt und Setup abgeschlossen haben, fahren Sie mit der Installation fort, indem Sie sich zum ersten Mal anmelden und einige Einstellungen konfigurieren.

Dieses Kapitel behandelt die folgenden Themen:

- „Über vRealize Operations Manager-Neuinstallationen“, auf Seite 33
- „Anmelden und Wiederaufnehmen einer Neuinstallation“, auf Seite 33

Über vRealize Operations Manager -Neuinstallationen

Eine vRealize Operations Manager-Neuinstallation setzt voraus, dass Sie Knoten bereitstellen und konfigurieren. Danach fügen Sie Lösungen für die Arten von Objekten hinzu, die Sie überwachen und verwalten.

Nachdem Sie Lösungen hinzugefügt haben, konfigurieren Sie sie im Produkt und fügen Überwachungsrichtlinien hinzu, die die von Ihnen gewünschten Daten erfassen.



Erstmaliges Anmelden (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vrops_first_time_login)

Anmelden und Wiederaufnehmen einer Neuinstallation

Zum Abschließen einer Neuinstallation von vRealize Operations Manager melden Sie sich an und führen einen einmaligen Prozess aus, um das Produkt zu lizenzieren und Lösungen für die Arten von Objekten zu konfigurieren, die Sie überwachen möchten.

Voraussetzungen

- Erstellen Sie den neuen Cluster von vRealize Operations Manager-Knoten.
- Überprüfen Sie, ob der Cluster ausreichend Kapazität zur Überwachung Ihrer Umgebung hat. Weitere Informationen hierzu finden Sie unter „Größenbestimmung des vRealize Operations Manager-Clusters“, auf Seite 15.

Vorgehensweise

- 1 Navigieren Sie in einem Web-Browser zu der IP-Adresse oder dem voll qualifizierten Domännennamen des Master-Knotens.
- 2 Geben Sie den Benutzernamen **admin** und das Kennwort ein, das Sie bei der Konfiguration des Master-Knotens definiert haben, und klicken Sie auf **Anmelden**.

Weil es sich dabei um Ihre erste Anmeldung handelt, wird die Verwaltungsschnittstelle geöffnet.

- 3 Um den Cluster zu starten, klicken Sie auf **vRealize Operations Manager starten**.

4 Klicken Sie auf **Ja**.

Abhängig von Ihrer Umgebung kann es 10 bis 30 Minuten dauern, bis der Cluster gestartet ist. Während der Cluster gestartet wird, nehmen Sie keine Änderungen an den Clusterknoten vor und führen Sie keine Aktionen auf sie aus.

5 Wenn der Startvorgang des Clusters abgeschlossen ist und die Seite zur Produktanmeldung angezeigt wird, geben Sie erneut den Benutzernamen und das Kennwort des Administrators ein und klicken Sie auf **Anmelden**.

Ein einmaliger Lizenzierungsassistent wird angezeigt.

6 Klicken Sie auf **Weiter**.7 Lesen und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie auf **Weiter**.

8 Geben Sie Ihren Produktschlüssel ein oder wählen Sie die Option zum Ausführen von vRealize Operations Manager im Testmodus aus.

Ihre Produktlizenzstufe bestimmt, welche Lösungen Sie installieren können, um Objekte zu überwachen und zu verwalten.

- Standard. Nur vCenter
- Erweitert. vCenter sowie andere Infrastrukturlösungen
- Enterprise. Alle Lösungen

vRealize Operations Manager lizenziert verwaltete Objekte nicht so, wie dies bei vSphere der Fall ist, weshalb bei der Produktlizenzierung die Anzahl der Objekte nicht verfügbar ist.

HINWEIS Nach dem Übergang auf die Standardedition stehen Ihnen die Funktionen der Advanced-Edition und der Enterprise-Edition nicht mehr zur Verfügung. Löschen Sie nach dem Übergang sämtliche in den anderen Versionen erstellte Inhalte, um sicherzustellen, dass die Lizenzvereinbarung eingehalten wird, und überprüfen Sie den Lizenzschlüssel, der die Funktionen der Advanced- und der Enterprise-Edition unterstützt.

9 Falls Sie einen Produktschlüssel eingegeben haben, klicken Sie auf **Lizenzschlüssel validieren**.10 Klicken Sie auf **Weiter**.11 Wählen Sie aus, ob Nutzungsstatistiken an VMware zurückgegeben werden sollen, und klicken Sie auf **Weiter**.12 Klicken Sie auf **Beenden**.

Der einmalige Assistent wird beendet, und die vRealize Operations Manager-Schnittstelle wird angezeigt.

Weiter

- Verwenden Sie die vRealize Operations Manager-Schnittstelle zum Konfigurieren der mit diesem Produkt mitgelieferten Lösungen.
- Verwenden Sie die vRealize Operations Manager-Schnittstelle, um weitere Lösungen hinzuzufügen.
- Fügen Sie mithilfe der vRealize Operations Manager-Schnittstelle Überwachungsrichtlinien hinzu.

Verbinden von vRealize Operations Manager mit Datenquellen

7

Konfigurieren Sie in vRealize Operations Manager Lösungen für den Verbindungsaufbau zu und die Analyse von Daten aus externen Datenquellen in Ihrer Umgebung. Sobald die Verbindung hergestellt wurde, verwenden Sie vRealize Operations Manager zum Überwachen und Verwalten von Objekten in Ihrer Umgebung.

Eine Lösung ist möglicherweise nur eine Verbindung zu einer Datenquelle; die Lösung kann aber auch vordefinierte Dashboards, Widgets, Warnungen und Ansichten enthalten.

vRealize Operations Manager beinhaltet die Lösungen VMware vSphere und Endpoint Operations Management. Diese Lösungen werden mit dem Installieren von vRealize Operations Manager installiert.

Weitere Lösungen können dem vRealize Operations Manager als Managementpakete hinzugefügt werden, z. B. das VMware Management Pack für NSX für vSphere. Um VMware-Managementpakete und andere Lösungen von Drittanbietern herunterzuladen, besuchen Sie [VMware Solution Exchange](#).

Dieses Kapitel behandelt die folgenden Themen:

- „[VMware vSphere Lösung in vRealize Operations Manager](#)“, auf Seite 35
- „[Endpoint Operations Management Lösung in vRealize Operations Manager](#)“, auf Seite 39
- „[Installieren optionaler Lösungen in vRealize Operations Manager](#)“, auf Seite 81
- „[Migrieren einer vCenter Operations Manager-Bereitstellung in diese Version](#)“, auf Seite 83

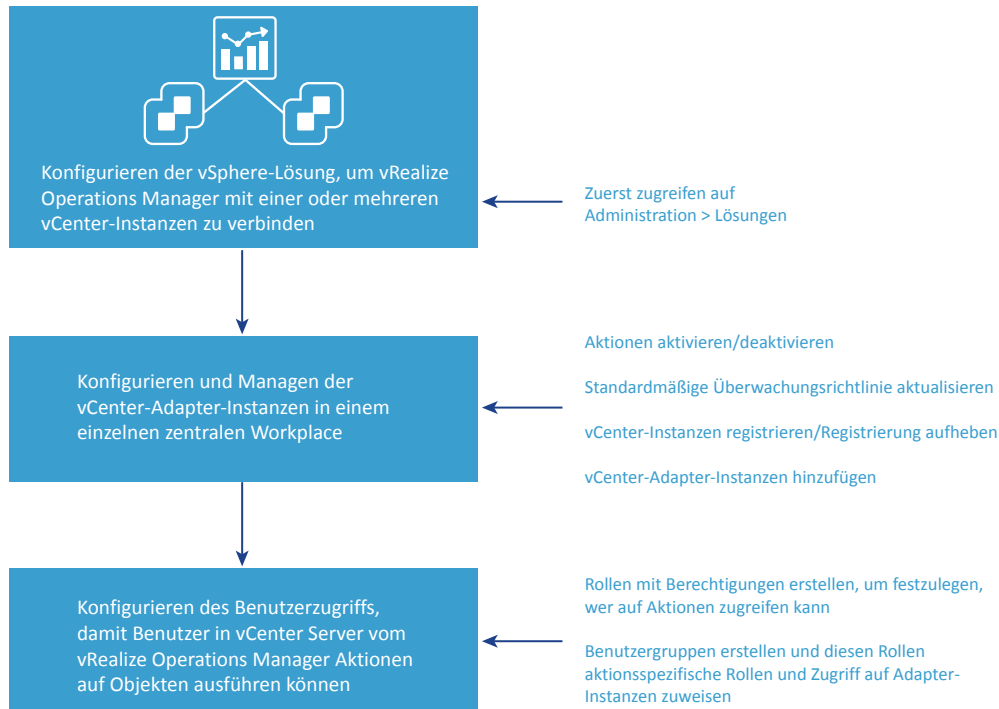
VMware vSphere Lösung in vRealize Operations Manager

Die VMware vSphere-Lösung stellt eine Verbindung zwischen vRealize Operations Manager und vCenter Server-Instanzen her. Erfassen Sie Daten von diesen Instanzen und Metriken, überwachen Sie diese Instanzen, und führen Sie in diesen Instanzen Aktionen aus.

vRealize Operations Manager wertet die Daten in Ihrer Umgebung aus, indem Trends im Objektverhalten ermittelt, mögliche Probleme und zukünftige Kapazitäten für Objekte in Ihrem System basierend auf diesen Trends berechnet und Warnungen an Sie ausgegeben werden, wenn ein Objekt definierte Symptome aufweist.

Konfigurieren der vSphere-Lösung

Die vSphere-Lösung ist zusammen mit vRealize Operations Manager installiert. Sie enthält den vCenter Server-Adapter, den Sie konfigurieren müssen, um vRealize Operations Manager an Ihre vCenter Server-Instanzen anzuschließen.



Funktionsweise der Anmeldedaten für Adapter

Die Anmeldedaten für vCenter Server, die Sie zum Verbinden von vRealize Operations Manager mit einer vCenter Server-Instanz verwenden, legen die Objekte fest, die vRealize Operations Manager überwacht. Machen Sie sich mit der Art und Weise der Interaktionen dieser Adapter-Anmeldedaten und Benutzerrechte vertraut. Nur so ist sichergestellt, dass Sie Adapter und Benutzer korrekt konfigurieren. Außerdem werden dadurch einige der folgenden Probleme vermieden.

- Wenn Sie den Adapter für eine Verbindung zu einer vCenter Server-Instanz mit Anmeldedaten konfigurieren, die nur Berechtigung für den Zugriff auf einen einzigen Ihrer drei Hosts haben, sieht jeder Benutzer, der sich an vRealize Operations Manager anmeldet, nur diesen einen Host, auch dann, wenn der einzelne Benutzer die Berechtigung für alle drei Hosts in vCenter Server hat.
- Wenn die zur Verfügung gestellten Anmeldedaten nur eingeschränkten Zugriff auf Objekte in vCenter Server bieten, können selbst Administratoren in vRealize Operations Manager Aktionen nur für die Objekte ausführen, für die die vCenter Server-Anmeldedaten Berechtigungen haben.
- Wenn die zur Verfügung gestellten Anmeldedaten über Zugriff auf alle Objekte in vCenter Server verfügen, kann jeder vRealize Operations Manager-Benutzer, der Aktionen ausführt, dieses Konto nutzen.

Steuern des Benutzerzugriffs auf Aktionen

Der vCenter-Serveradapter enthält Aktionen, die Sie auf dem vCenter-Server von vRealize Operations Manager ausführen können. Wenn Sie wählen, Aktionen auszuführen, müssen Sie den Benutzerzugriff steuern. Sie steuern den Benutzerzugriff für lokale Benutzer über die Konfiguration der Benutzerrechte in vRealize Operations Manager. Für Benutzer, die sich über ihr vCenter Server-Konto anmelden, werden ihre Rechte über die Art und Weise der Konfiguration ihres Kontos in vCenter Server bestimmt.

So haben Sie beispielsweise einen vCenter Server-Benutzer mit Lesezugriff in vCenter Server. Wenn Sie diesem Benutzer die vRealize Operations Manager-Power-User-Rolle in vCenter Server anstatt eine mehr eingeschränkte Rolle zuweisen, kann er Aktionen für Objekte ausführen, da der Adapter mit Anmeldedaten konfiguriert wird, die das Recht zum Verändern von Objekten beinhalten. Um diese Situationen zu vermeiden, konfigurieren Sie vRealize Operations Manager-Benutzer und vCenter Server-Benutzer mit den Berechtigungen, die Sie in Ihrer Umgebung haben sollen.

Hinzufügen einer vCenter-Adapterinstanz in vRealize Operations Manager

Für die Verwaltung Ihrer vCenter Server-Instanzen in vRealize Operations Manager müssen Sie für jede vCenter Server-Instanz eine Adapterinstanz konfigurieren. Der Adapter benötigt die Anmeldedaten, die für die Kommunikation mit dem Ziel-vCenter Server verwendet werden.



VORSICHT Alle Adapter-Anmeldedaten, die Sie hinzufügen, werden mit anderen Adapter-Administratoren und vRealize Operations Manager-Collector-Hosts gemeinsam genutzt. Andere Administratoren können diese Anmeldedaten verwenden, um eine neue Adapterinstanz zu konfigurieren oder eine Adapterinstanz auf einen neuen Host zu verschieben.



Konfigurieren der vSphere-Lösung (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_config_vsphere_solution)

Voraussetzungen

Stellen Sie sicher, dass die Anmeldedaten für vCenter Server über die erforderlichen Berechtigungen für die Verbindungsherstellung und die Datenerfassung verfügen. Wenn der Zugriff auf Objekte in vCenter Server mit den eingegebenen Anmeldedaten beschränkt ist, werden allen Benutzern, unabhängig von ihren vCenter Server-Rechten, nur die Objekte in Übereinstimmung mit den eingegebenen Anmeldedaten angezeigt. Das Benutzerkonto muss mindestens über Leseberechtigungen verfügen und die Zuweisung der Leseberechtigungen muss auf der Rechenzentrums- oder vCenter Server-Ebene erfolgt sein.

Vorgehensweise

- 1 Klicken Sie im linken Bereich von vRealize Operations Manager auf das Symbol **Verwaltung** und klicken Sie dann auf **Lösungen**.
- 2 Wählen Sie auf der Registerkarte **Lösungen** die Option **VMware vSphere** aus und klicken Sie auf der Registerkarte auf **Konfigurieren**.
- 3 Geben Sie einen Anzeigenamen und eine Beschreibung für die Adapterinstanz ein.
- 4 Geben Sie im Textfeld **vCenter Server** den FQDN oder die IP-Adresse der vCenter Server-Instanz ein, mit der Sie eine Verbindung herstellen.

Der FQDN oder die IP-Adresse von vCenter Server muss von allen Knoten im vRealize Operations Manager-Cluster aus erreichbar sein.

- 5 Um die Anmeldedaten für die vCenter Server-Instanz hinzuzufügen, klicken Sie auf das Symbol **Hinzufügen**, und geben Sie die erforderlichen Anmeldedaten ein.

- 6 Der Adapter ist auf das Ausführen von Aktionen in vCenter Server vom vRealize Operations Manager konfiguriert. Wenn Sie keine Aktionen ausführen möchten, wählen Sie **Deaktivieren** aus.

Die für die vCenter Server-Instanz angegebenen Anmeldedaten werden ebenfalls für das Ausführen von Aktionen verwendet. Wenn Sie diese Anmeldedaten nicht verwenden möchten, können Sie alternative Anmeldedaten vorgeben. Erweitern Sie dazu **Alternative Anmeldedaten für Aktionen**, und klicken Sie auf das Symbol **Hinzufügen**.
- 7 Klicken Sie auf **Testverbindung**, um die Verbindung mit der vCenter Server-Instanz zu validieren.
- 8 Überprüfen Sie im Dialogfeld Review and Accept Certificate (Zertifikat überprüfen und annehmen) die Zertifikatsinformationen.
 - ◆ Wenn das im Dialogfeld dargestellte Zertifikat mit dem Zertifikat Ihrer vCenter Server-Zielinstanz übereinstimmt, klicken Sie auf **OK**.
 - ◆ Falls das Zertifikat nicht gültig ist, klicken Sie auf **Cancel** (Abbrechen). Der Test schlägt fehl und die Verbindung mit vCenter Server wird nicht hergestellt. Sie müssen eine gültige vCenter Server-URL angeben oder sicherstellen, dass das Zertifikat auf vCenter Server gültig ist, bevor Sie die Adapterkonfiguration abschließen.
- 9 Um die erweiterten Optionen in Bezug auf Collectoren, Objekterkennung oder Änderungsereignisse zu ändern, erweitern Sie **Erweiterte Einstellungen**.
- 10 Um die standardmäßige Überwachungsrichtlinie anzupassen, die vRealize Operations Manager für die Analyse und das Anzeigen von Informationen über die Objekte in Ihrer Umgebung verwendet wird, klicken Sie auf **Überwachungsziele definieren**.

Wenn Sie benutzerdefinierte Anpassungen an dieser Richtlinie vornehmen möchten, greifen Sie auf der Seite **Richtlinien** auf diese Richtlinie zu.
- 11 Um die Registrierung von vCenter-Instanzen zu verwalten, klicken Sie auf **Registrierungen verwalten**.

Sie können alternative Anmeldedaten vorgeben oder das Kontrollkästchen **Anmeldedaten für Erfassung verwenden** aktivieren, die beim Konfigurieren dieser vCenter Server-Adapterinstanz angegeben wurden.
- 12 Klicken Sie auf **Einstellungen speichern**.

Die Adapterinstanz wird zur Liste hinzugefügt.

vRealize Operations Manager beginnt mit der Datenerfassung für die vCenter Server-Instanz. Je nach der Anzahl der verwalteten Objekte kann die anfängliche Erfassung mehr als einen Erfassungszyklus dauern. Alle fünf Minuten beginnt ein Standarderfassungszyklus.

Weiter

Wenn Sie den Adapter auf das Ausführen von Aktionen konfiguriert haben, konfigurieren Sie einen Benutzerzugriff für diese Aktionen, indem Sie Aktionsrollen und Benutzergruppen erstellen.

Konfigurieren des Benutzerzugriffs für Aktionen

Zum Ausführen von Aktionen in vRealize Operations Manager durch Benutzer müssen Sie den Benutzerzugriff für die Aktionen konfigurieren.

Über Rollenberechtigungen können Sie die Aktionen bestimmen, die Benutzer ausführen dürfen. Sie können mehrere Rollen erstellen. Mit jeder Rolle können Benutzer Berechtigungen zur Ausführung verschiedener Teilmengen von Aktionen erhalten. Benutzer, die die Administratorrolle oder die Standardrolle „Superuser“ innehaben, verfügen bereits über die erforderlichen Berechtigungen zum Ausführen von Aktionen.

Sie können Benutzergruppen erstellen, um einer Gruppe aktionsspezifische Rollen hinzuzufügen, statt einzelne Benutzerrechte zu konfigurieren.

Vorgehensweise

- 1 Klicken Sie im linken Fensterbereich von vRealize Operations Manager auf **Administration > Zugriffssteuerung**.
- 2 So erstellen Sie eine Rolle:
 - a Klicken Sie auf die Registerkarte **Rollen**.
 - b Klicken Sie auf das Symbol **Hinzufügen** und geben Sie dann einen Namen und eine Beschreibung für die Rolle ein.
- 3 Um der Rolle Berechtigungen hinzuzufügen, wählen Sie die Rolle aus und klicken Sie dann im Berechtigungsbereich auf das Symbol **Bearbeiten**.
 - a Erweitern Sie **Umgebung** und anschließend **Aktion**.
 - b Wählen Sie eine oder mehrere Aktionen aus und klicken Sie auf **Aktualisieren**.
- 4 So erstellen Sie eine Benutzergruppe:
 - a Klicken Sie auf die Registerkarte **Benutzergruppen** und dann auf das Symbol **Benutzergruppe hinzufügen**.
 - b Geben Sie einen Namen und eine Beschreibung für die Gruppe ein und klicken Sie dann auf **Weiter**.
 - c Weisen Sie der Gruppe Benutzer zu und klicken Sie auf die Registerkarte **Objekte**.
 - d Wählen Sie eine Rolle aus, die mit Berechtigungen zum Ausführen von Aktionen erstellt wurde, und aktivieren Sie dann das Kontrollkästchen **Dem Benutzer diese Roll zuweisen**.
 - e Konfigurieren Sie die Objektberechtigungen, indem Sie jede Adapterinstanz auswählen, zu der die Gruppe Zugriff benötigt, um Aktionen auszuführen.
 - f Klicken Sie auf **Beenden**.

Weiter

Testen Sie die Benutzer, die Sie der Gruppe zugeordnet haben. Melden Sie sich ab und melden Sie sich dann als einer der Benutzer wieder an. Überprüfen Sie, ob dieser Benutzer die erwarteten Aktionen auf dem ausgewählten Adapter ausführen kann.

Endpoint Operations Management Lösung in vRealize Operations Manager

Sie konfigurieren Endpoint Operations Management, um Betriebssystem-Metriken zu erfassen und die Verfügbarkeit der Remote-Plattformen und Anwendungen zu überwachen. Diese Lösung wird mit vRealize Operations Manager installiert.

Installation und Bereitstellung des Endpoint Operations Management -Agenten

Verwenden Sie die Informationen in diesen Links als Hilfe bei der Installation und Bereitstellung von Endpoint Operations Management-Agenten in Ihrer Umgebung.

Vorbereitung der Installation des Endpoint Operations Management -Agenten

Bevor Sie den Endpoint Operations Management-Agenten installieren, müssen Sie vorbereitende Schritte ausführen.

Voraussetzungen

- Um den Agenten so zu konfigurieren, dass er einen von Ihnen selbst verwalteten Keystore für SSL-Kommunikation verwendet, richten Sie für den Agenten auf seinem Host einen Keystore im JKS-Format ein und importieren Sie sein SSL-Zertifikat. Notieren Sie sich den vollständigen Pfad zum Keystore sowie sein Kennwort. Diese Daten müssen Sie in der Datei `agent.properties` des Agenten angeben.

Prüfen Sie, ob das Kennwort für den Agenten-Keystore und das private Schlüsselkennwort identisch sind.

- Definieren Sie den `HQ_JAVA_HOME`-Speicherort des Agenten.

Plattformspezifische vRealize Operations Manager-Installationsprogramme enthalten JRE 1.8.x. Abhängig von Ihrer Umgebung und dem verwendeten Installationsprogramm müssen Sie unter Umständen den Speicherort der JRE angeben, um sicherzustellen, dass der Agent die zu verwendende JRE findet. Weitere Informationen hierzu finden Sie unter „[Konfigurieren von JRE-Speicherorten für Endpoint Operations Management-Komponenten](#)“, auf Seite 47.

Unterstützte Betriebssysteme für den Endpoint Operations Management -Agenten

In diesen Tabellen werden die unterstützten Betriebssysteme für die Bereitstellung des Endpoint Operations Management-Agenten beschrieben.

Diese Konfigurationen werden für den Agenten in Entwicklungs- und Produktionsumgebungen unterstützt.

Tabelle 7-1. Unterstützte Betriebssysteme für den Endpoint Operations Management -Agenten

Betriebssystem	Prozessorarchitektur	JVM
RedHat Enterprise Linux (RHEL) 5.x, 6.x, 7.x	x86_64, x86_32	Oracle Java SE8
CentOS 5.x, 6.x, 7.x	x86_64, x86_32	Oracle Java SE8
SUSE Enterprise Linux (SLES) 11.x, 12.x	x86_64	Oracle Java SE8
Windows 2008 Server, 2008 Server R2	x86_64, x86_32	Oracle Java SE8
Windows 2012 Server, 2012 Server R2	x86_64	Oracle Java SE8
Solaris 10, 11	x86_64, SPARC	Oracle Java SE7
AIX 6.1, 7.1	Power PC	IBM Java SE7
VMware Photon Linux 1.0	x86_64	OpenJDK 1.8.0_72-BLFS
Oracle Linux, Versionen 5, 6, 7	x86_64, x86_32	OpenJDK Runtime Environment 1.7

Auswählen eines Agenteninstallationspakets

Die Installationsdateien für den Endpoint Operations Management-Agenten sind im vRealize Operations Manager-Installationspaket enthalten.

Sie können den Endpoint Operations Management-Agenten mit einem `tar.gz`- oder `.zip`-Archiv installieren oder über ein spezifisches Installationsprogramm für Windows- oder Linux-Systeme, die RPM unterstützen.

Hinweis: Wenn Sie eine Nicht-JRE-Version des Endpoint Operations Management-Agenten installieren, empfiehlt VMware die Verwendung ausschließlich der neuesten Java-Version, um Sicherheitsrisiken im Zusammenhang mit Java-Versionen zu vermeiden.

- [Installieren des Agenten auf einer Linux-Plattform aus einem RPM-Paket](#) auf Seite 41
Sie können den Endpoint Operations Management-Agenten aus einem RedHat Package Manager-Paket (RPM-Paket) installieren. Der Agent im noarch-Paket umfasst keine JRE.
- [Installieren des Agenten auf einer Linux-Plattform aus einem Archiv](#) auf Seite 43
Sie können einen Endpoint Operations Management-Agenten auf einer Linux-Plattform aus einem tar.gz-Archiv installieren.
- [Installieren des Agenten auf einer Windows-Plattform aus einem Archiv](#) auf Seite 44
Sie können einen Endpoint Operations Management-Agenten auf einer Windows-Plattform aus einer .zip-Datei installieren.
- [Installieren des Agenten auf einer Windows-Plattform mit dem Windows-Installationsprogramm](#) auf Seite 44
Sie können den Endpoint Operations Management-Agenten auf einer Windows-Plattform mit einem Windows-Installationsprogramm installieren.
- [Unbeaufsichtigte Installation eines Endpoint Operations Management-Agenten auf einem Windows-Computer](#) auf Seite 46
Sie können einen Endpoint Operations Management-Agenten auf einem Windows-Computer unbeaufsichtigt oder vollkommen unbeaufsichtigt installieren.

Installieren des Agenten auf einer Linux-Plattform aus einem RPM-Paket

Sie können den Endpoint Operations Management-Agenten aus einem RedHat Package Manager-Paket (RPM-Paket) installieren. Der Agent im noarch-Paket umfasst keine JRE.

Archive ausschließlich für Agenten sind hilfreich, wenn Sie Agenten für eine große Anzahl von Plattformen für unterschiedliche Betriebssysteme und Architekturen bereitstellen. Agentenarchive sind für Windows- und UNIX-Umgebungen mit und ohne integrierte JREs verfügbar.

Der RPM führt folgende Aktionen aus:

- Erstellt einen Benutzer und eine Gruppe mit der Bezeichnung epops, falls nicht vorhanden. Der Benutzer ist ein gesperrtes Servicekonto, bei dem Sie sich nicht anmelden können.
- Installiert die Agentendateien unter /opt/vmware/epops-agent.
- Installiert ein Init-Skript unter /etc/init.d/epops-agent.
- Für das init-Skript zu chkconfig hinzu und legt es für Ablaufebenen 2, 3, 4 und 5 auf on fest.

Wenn mehrere Agenten installiert werden müssen, siehe „[Gleichzeitiges Installieren mehrerer Endpoint Operations Management-Agenten](#)“, auf Seite 75.

Voraussetzungen

- Prüfen Sie, ob Sie über ausreichend Berechtigungen verfügen, um einen Endpoint Operations Management-Agenten bereitzustellen. Sie müssen vRealize Operations Manager-Benutzeranmeldeinformationen haben, die die Rolle umfassen, mit der Sie Endpoint Operations Management-Agenten installieren können. Weitere Informationen hierzu finden Sie unter „[Rollen und Berechtigungen in vRealize Operations Manager](#)“, auf Seite 78.
- Wenn Sie planen, ICMP-Überprüfungen auszuführen, müssen Sie den Endpoint Operations Management-Agenten mit **root**-Berechtigungen installieren.

- Um den Agenten so zu konfigurieren, dass er einen von Ihnen selbst verwalteten Keystore für SSL-Kommunikation verwendet, richten Sie für den Agenten auf seinem Host einen Keystore im JKS-Format ein und konfigurieren Sie den Agenten zur Verwendung des SSL-Zertifikats. Notieren Sie sich den vollständigen Pfad zum Keystore sowie sein Kennwort. Diese Daten müssen Sie in der Datei `agent.properties` des Agenten angeben.

Prüfen Sie, ob das Kennwort für den Agenten-Keystore und das private Schlüsselkennwort identisch sind.

- Wenn Sie ein Nicht-JRE-Paket installieren, definieren Sie den `HQ_JAVA_HOME`-Speicherort des Agenten.
Für die Endpoint Operations Management-Plattform spezifische Installationsprogramme enthalten JRE 1.8.x, Plattformunabhängige Installationsprogramme nicht. Abhängig von Ihrer Umgebung und dem verwendeten Installationsprogramm müssen Sie unter Umständen den Speicherort der JRE angeben, um sicherzustellen, dass der Agent die zu verwendende JRE findet. Weitere Informationen hierzu finden Sie unter „[Konfigurieren von JRE-Speicherorten für Endpoint Operations Management-Komponenten](#)“, auf Seite 47.
- Wenn Sie ein anderes Paket als ein JRE-Paket installieren, vergewissern Sie sich, dass Sie die letzten Java-Version verwenden. Bei Verwendung von früheren Versionen von Java setzen Sie sich potenziellen Sicherheitsrisiken aus.
- Stellen Sie sicher, dass das Installationsverzeichnis für den Endpoint Operations Management-Agenten keine vRealize Hyperic-Agenteninstallation enthält.
- Wenn Sie die noarch-Installation verwenden, prüfen Sie, ob auf der Plattform ein JDK oder eine JRE installiert ist.
- Stellen Sie sicher, dass Sie bei der Angabe des Installationspfads für den Agenten nur ASCII-Zeichen verwenden. Wenn Sie Nicht-ASCII-Zeichen verwenden möchten, müssen Sie die Codierung der Linux-Maschine und SSH-Client-Anwendung auf UTF-8 festlegen.

Vorgehensweise

- 1 Laden Sie das entsprechende RPM-Paket auf die Zielmaschine herunter.

Betriebssystem	RPM-Paket zum Herunterladen
64-Bit-Betriebssystem	<code>epops-agent-x86-64-linux-version.rpm</code>
32-Bit-Betriebssystem	<code>epops-agent-x86-linux-version.rpm</code>
Kein Archiv	<code>epops-agent-noarch-linux-version.rpm</code>

- 2 Öffnen Sie mit `root`-Anmeldedaten eine SSH-Verbindung.
- 3 Führen Sie `rpm -i epops-agent-Arch-linux-version.rpm` aus, um den Agenten auf der Plattform zu installieren, die der Agent überwachen soll, wobei *Arch* der Name des Archivs und *version* die Versionsnummer ist.

Der Endpoint Operations Management-Agent wird installiert und der Service wird so konfiguriert, dass er beim Systemstart gestartet wird.

Weiter

Bevor Sie den Service starten, vergewissern Sie sich, dass die Anmeldedaten des `epops`-Benutzers alle Berechtigungen enthalten, die erforderlich sind, damit Ihre Plug-ins die entsprechenden Anwendungen erkennen und überwachen können. Führen Sie anschließend eine der folgenden Prozesse aus.

- Führen Sie `service epops-agent start` aus, um den `epops-agent`-Service zu starten.
- Wenn Sie den Endpoint Operations Management-Agenten auf einer Maschine mit SuSE 12.x installiert haben, starten Sie den Endpoint Operations Management-Agenten mit dem Befehl `[EP Ops Home]/bin/ep-agent.sh start`.

- Wenn Sie versuchen, einen Endpoint Operations Management-Agenten zu starten, wird eventuell die Meldung angezeigt, dass der End Point Operations Manager-Agent bereits ausgeführt wird. Führen Sie vor dem Start des Agenten den folgenden Befehl aus: `./bin/ep-agent.sh stop`.
- Konfigurieren Sie den Agenten in der Datei `agent.properties` und starten Sie anschließend den Service. Weitere Informationen hierzu finden Sie unter „[Endpoint Operations Management-Agenten-zu-vRealize Operations Manager-Server-Konfigurationseigenschaften aktivieren](#)“, auf Seite 50.

Installieren des Agenten auf einer Linux-Plattform aus einem Archiv

Sie können einen Endpoint Operations Management-Agenten auf einer Linux-Plattform aus einem `tar.gz`-Archiv installieren.

Der Konfigurationsvorgang fordert Sie während der Installation standardmäßig auf, die Konfigurationswerte einzugeben. Sie können diesen Vorgang automatisieren, indem Sie die Werte in der Agenteneigenschaftsdatei festlegen. Wenn das Installationsprogramm Werte in der Eigenschaftsdatei erkennt, werden diese Werte angewendet. Nachfolgende Bereitstellungen verwenden auch die in der Agenteneigenschaftsdatei angegebenen Werte.

Voraussetzungen

- Prüfen Sie, ob Sie über ausreichend Berechtigungen verfügen, um einen Endpoint Operations Management-Agenten bereitzustellen. Sie müssen vRealize Operations Manager-Benutzeranmeldeinformationen haben, die die Rolle umfassen, mit der Sie Endpoint Operations Management-Agenten installieren können. Weitere Informationen hierzu finden Sie unter „[Rollen und Berechtigungen in vRealize Operations Manager](#)“, auf Seite 78.
- Wenn Sie planen, ICMP-Überprüfungen auszuführen, müssen Sie den Endpoint Operations Management-Agenten mit **root**-Berechtigungen installieren.
- Stellen Sie sicher, dass das Installationsverzeichnis für den Endpoint Operations Management-Agenten keine vRealize Hyperic-Agenteninstallation enthält.
- Stellen Sie sicher, dass Sie bei der Angabe des Installationspfads für den Agenten nur ASCII-Zeichen verwenden. Wenn Sie Nicht-ASCII-Zeichen verwenden möchten, müssen Sie die Codierung der Linux-Maschine und SSH-Client-Anwendung auf UTF-8 festlegen.

Vorgehensweise

- 1 Laden Sie die Installationsdatei `tar.gz` des Endpoint Operations Management-Agenten herunter, die für Ihr Linux-Betriebssystem geeignet ist.

Betriebssystem	tar.gz-Paket zum Herunterladen
64-Bit-Betriebssystem	<code>epops-agent-x86-64-linux-version.tar.gz</code>
32-Bit-Betriebssystem	<code>epops-agent-x86-linux-version.tar.gz</code>
Kein Archiv	<code>epops-agent-noJRE-version.tar.gz</code>

- 2 Führen Sie `cd agent name/bin` aus, um das bin-Verzeichnis für den Agenten zu öffnen.
- 3 Führen Sie `ep-agent.sh start` aus.

Wenn Sie zum ersten Mal einen Agenten installieren, startet der Befehl den Konfigurationsvorgang, sofern Sie alle erforderlichen Konfigurationswerte nicht in der Agenteneigenschaftsdatei festgelegt haben.
- 4 (Optional) Rufen Sie `ep-agent.sh status` auf, um den aktuellen Status des Agenten, einschließlich IP-Adresse und Port, anzuzeigen.

Weiter

Registrieren Sie das Client-Zertifikat für den Agenten. Weitere Informationen hierzu finden Sie unter „[Regenerieren des Clientzertifikats eines Agenten](#)“, auf Seite 70.

Installieren des Agenten auf einer Windows-Plattform aus einem Archiv

Sie können einen Endpoint Operations Management-Agenten auf einer Windows-Plattform aus einer .zip-Datei installieren.

Der Konfigurationsvorgang fordert Sie während der Installation standardmäßig auf, die Konfigurationswerte einzugeben. Sie können diesen Vorgang automatisieren, indem Sie die Werte in der Agenteneigenschaftsdatei festlegen. Wenn das Installationsprogramm Werte in der Eigenschaftsdatei erkennt, werden diese Werte angewendet. Nachfolgende Bereitstellungen verwenden auch die in der Agenteneigenschaftsdatei angegebenen Werte.

Voraussetzungen

- Prüfen Sie, ob Sie über ausreichend Berechtigungen verfügen, um einen Endpoint Operations Management-Agenten bereitzustellen. Sie müssen vRealize Operations Manager-Benutzeranmeldeinformationen haben, die die Rolle umfassen, mit der Sie Endpoint Operations Management-Agenten installieren können. Weitere Informationen hierzu finden Sie unter „[Rollen und Berechtigungen in vRealize Operations Manager](#)“, auf Seite 78.
- Stellen Sie sicher, dass das Installationsverzeichnis für den Endpoint Operations Management-Agenten keine vRealize Hyperic-Agenteninstallation enthält.
- Prüfen Sie, ob ein Endpoint Operations Management- oder vRealize Hyperic-Agent in Ihrer Umgebung installiert ist, bevor Sie das Windows-Installationsprogramm ausführen.

Vorgehensweise

- 1 Laden Sie die .zip-Installationsdatei des Endpoint Operations Management-Agenten herunter, die für Ihr Windows-Betriebssystem geeignet ist.

Betriebssystem	ZIP-Paket zum Herunterladen
64-Bit-Betriebssystem	epops-agent-x86-64-win-version.zip
32-Bit-Betriebssystem	epops-agent-win32-version.zip
Kein Archiv	epops-agent-noJRE-version.zip

- 2 Führen Sie `cd agent name\bin` aus, um das bin-Verzeichnis für den Agenten zu öffnen.
- 3 Führen Sie `ep-agent.bat install` aus.
- 4 Führen Sie `ep-agent.bat start` aus.

Wenn Sie zum ersten Mal einen Agenten installieren, startet der Befehl den Konfigurationsvorgang, sofern Sie die Konfigurationswerte nicht in der Agenteneigenschaftsdatei festgelegt haben.

Weiter

Generieren Sie das Client-Zertifikat für den Agenten. Weitere Informationen hierzu finden Sie unter „[Regenerieren des Clientzertifikats eines Agenten](#)“, auf Seite 70.

Installieren des Agenten auf einer Windows-Plattform mit dem Windows-Installationsprogramm

Sie können den Endpoint Operations Management-Agenten auf einer Windows-Plattform mit einem Windows-Installationsprogramm installieren.

Sie können eine unbeaufsichtigte Installation des Agenten durchführen. Weitere Informationen hierzu finden Sie unter „[Unbeaufsichtigte Installation eines Endpoint Operations Management-Agenten auf einem Windows-Computer](#)“, auf Seite 46.

Voraussetzungen

- Prüfen Sie, ob Sie über ausreichend Berechtigungen verfügen, um einen Endpoint Operations Management-Agenten bereitzustellen. Sie müssen vRealize Operations Manager-Benutzeranmeldeinformationen haben, die die Rolle umfassen, mit der Sie Endpoint Operations Management-Agenten installieren können. Weitere Informationen hierzu finden Sie unter „[Rollen und Berechtigungen in vRealize Operations Manager](#)“, auf Seite 78.
- Stellen Sie sicher, dass das Installationsverzeichnis für den Endpoint Operations Management-Agenten keine vRealize Hyperic-Agenteninstallation enthält.
- Wenn auf der Maschine bereits ein Endpoint Operations Management-Agent installiert ist, prüfen Sie, dass er nicht ausgeführt wird.
- Prüfen Sie, ob ein Endpoint Operations Management- oder vRealize Hyperic-Agent in Ihrer Umgebung installiert ist, bevor Sie das Windows-Installationsprogramm ausführen.
- Sie müssen den Benutzernamen und das Kennwort für den vRealize Operations Manager, die vRealize Operations Manager-Serveradresse (FQDN) und den Fingerabdruckwert des Serverzertifikats kennen. Weitere Informationen zum Fingerabdruck des Zertifikats finden Sie in der Vorgehensweise.

Vorgehensweise

- 1 Laden Sie die EXE-Datei für die Windows-Installation herunter, die für Ihre Windows-Plattform geeignet ist.

Betriebssystem	RPM-Paket zum Herunterladen
64-Bit-Betriebssystem	<code>epops-agent-x86-64-win-version.exe</code>
32-Bit-Betriebssystem	<code>epops-agent-x86-win-version.exe</code>

- 2 Doppelklicken Sie auf die Datei, um den Installationsassistenten zu öffnen.
- 3 Führen Sie die Schritte im Installationsassistenten aus.

Prüfen Sie, ob das Gebietsschema des Benutzers mit dem des Systems identisch ist, und stellen Sie sicher, dass der Installationspfad nur Zeichen enthält, die Teil der Codeseite des Gebietsschemas sind. Sie können das Gebietsschema für Benutzer und System in den Einstellungen zu Region und Sprache in der Systemsteuerung festlegen.

Beachten Sie die folgenden Informationen zum Definieren des Fingerabdrucks des Serverzertifikats.

- Der Fingerabdruck des Serverzertifikats ist erforderlich, um eine unbeaufsichtigte Installation durchzuführen.
 - Für den Fingerabdruck kann entweder der SHA1- oder der SHA256-Algorithmus verwendet werden.
 - Standardmäßig generiert der vRealize Operations Manager-Server ein selbstsigniertes CA-Zertifikat, das zum Signieren des Zertifikats aller Knoten im Cluster verwendet wird. In diesem Fall muss der Fingerabdruck der des CA-Zertifikats sein, damit der Agent mit allen Knoten kommuniziert.
 - Als vRealize Operations Manager-Administrator können Sie ein benutzerdefiniertes Zertifikat importieren, anstatt das standardmäßige zu verwenden. In diesem Fall müssen Sie als Wert für diese Eigenschaft einen Fingerabdruck festlegen, der diesem Zertifikat entspricht.
 - Um den Wert des Zertifikatsfingerabdrucks einzusehen, loggen Sie sich in die vRealize Operations Manager-Verwaltungsschnittstelle unter `https://IP-Adresse/admin` ein, und klicken Sie auf das **SSL Zertifikat**-Symbol rechts in der Menüleiste. Falls Sie das Originalzertifikat nicht durch ein angepasstes Zertifikat ersetzt haben, ist der zweite Fingerabdruck in der Liste der richtige. Falls Sie ein angepasstes Zertifikat hochgeladen haben, ist der erste Fingerabdruck in der Liste der richtige.
- 4 (Optional) Führen Sie `ep-agent.bat query` aus, um zu überprüfen, ob der Agent installiert ist und läuft.

Der Agent wird auf der Windows-Plattform ausgeführt.



VORSICHT Der Agent wird auch dann ausgeführt, wenn einige der Parameter, die Sie im Installationsassistenten angegeben haben, fehlen oder ungültig sind. Prüfen Sie die Dateien `wrapper.log` und `agent.log` im Verzeichnis `product installation path/log`, um sicherzustellen, dass keine Installationsfehler aufgetreten sind.

Unbeaufsichtigte Installation eines Endpoint Operations Management -Agenten auf einem Windows-Computer

Sie können einen Endpoint Operations Management-Agenten auf einem Windows-Computer unbeaufsichtigt oder vollkommen unbeaufsichtigt installieren.

Unbeaufsichtigte und vollkommen unbeaufsichtigte Installationen werden über eine Befehlszeilenoberfläche mit einer ausführbaren Setup-Installationsdatei durchgeführt.

Prüfen Sie, ob ein Endpoint Operations Management- oder vRealize Hyperic-Agent in Ihrer Umgebung installiert ist, bevor Sie das Windows-Installationsprogramm ausführen.

Verwenden Sie die folgenden Parameter, um den Installationsvorgang einzurichten. Weitere Informationen zu diesen Parametern finden Sie unter „[Festlegen der Endpoint Operations Management-Agenten-Konfigurationseigenschaften](#)“, auf Seite 50.



VORSICHT Die Parameter, die Sie für das Windows-Installationsprogramm festlegen, werden ohne Überprüfung an die Agentenkonfiguration weitergegeben. Wenn Sie eine falsche IP-Adresse oder falsche Anmeldedaten eingeben, kann der Endpoint Operations Management-Agent nicht starten.

Tabelle 7-2. Parameter für unbeaufsichtigte Befehlszeileninstallation

Parameter	Wert	Obligatorisch/Optional	Anmerkungen
<code>-serverAddress</code>	FQDN/IP-Adresse:	Obligatorisch	FQDN oder IP-Adresse des vRealize Operations Manager-Servers.
<code>-username</code>	String	Obligatorisch	
<code>-securePort</code>	Anzahl	Optional	Der Standardwert lautet 443.
<code>-password</code>	String	Obligatorisch	
<code>-serverCertificateThumbprint</code>	String	Obligatorisch	Der Fingerabdruck des vRealize Operations Manager-Serverzertifikats. Sie müssen den Fingerabdruck des Zertifikats in Anführungs- und Ausführungszeichen setzen, z. B. <code>-serverCertificateThumbprint "31:32:FA:1F:FD:78:1E:D8:9A:15:32:85:D7:FE:54:49:0A:1D:9F:6D"</code> .

Es gibt Parameter zum Definieren verschiedener anderer Attribute für den Installationsvorgang.

Tabelle 7-3. Zusätzliche Parameter für unbeaufsichtigte Befehlszeileninstallation

Parameter	Standardwert	Anmerkungen
/DIR	C:\ep-agent	Gibt den Installationspfad an. Im Installationspfad dürfen keine Leerzeichen verwendet werden und Sie müssen den Befehl /DIR und den Installationspfad mit einem Gleichheitszeichen verbinden, z. B. /DIR=C:\ep-agent.
/SILENT	Kein	Gibt an, dass die Installation unbeaufsichtigt ist. Bei einer unbeaufsichtigten Installation wird nur das Fortschrittsfenster angezeigt.
/VERYSILENT	Kein	Gibt an, dass die Installation vollständig unbeaufsichtigt ist. Bei einer vollständig unbeaufsichtigten Installation wird das Fortschrittsfenster nicht angezeigt, jedoch Fehlermeldungen sowie die Startaufforderung, sofern Sie diese nicht deaktiviert haben.

Java-Voraussetzungen für den Endpoint Operations Management -Agenten

Alle Endpoint Operations Management-Agenten erfordern, dass die Richtliniendateien Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction als Teil des Java-Pakets enthalten sind.

Die Richtliniendateien Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction sind in den Installationsoptionen des JRE Endpoint Operations Management-Agenten enthalten.

Sie können ein Endpoint Operations Management-Agenten-Paket ohne JRE-Dateien oder wahlweise JRE zu einem späteren Zeitpunkt installieren.

Wenn Sie eine Installationsoption ohne JRE auswählen, müssen Sie sicherstellen, dass Ihr Java-Paket die Richtliniendateien Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction enthalten, um die Registrierung des Endpoint Operations Management-Agenten zu ermöglichen. Wenn Sie eine Option ohne JRE auswählen und Ihr Datenpaket die Richtliniendateien Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction nicht enthält, werden die Fehlermeldungen `Server ist möglicherweise heruntergefahren` (oder `falsche IP/falscher Port wurde verwendet`) und `TLS_RSA_WITH_AES_256_CBC_SHA` kann mit aktuell installierten Anbietern nicht unterstützt werden angezeigt.

Konfigurieren von JRE-Speicherorten für Endpoint Operations Management -Komponenten

Endpoint Operations Management-Agenten erfordern eine JRE. Die plattformspezifischen Endpoint Operations Management-Agenteninstallationsprogramme enthalten eine JRE. Plattformunabhängige Endpoint Operations Management-Agenteninstallationsprogramme enthalten keine JRE.

Wenn Sie eine Installationsoption ohne JRE auswählen, müssen Sie sicherstellen, dass Ihr Java-Paket die Richtliniendateien für Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction enthält, um die Registrierung des End Point Operations Management-Agenten zu ermöglichen. Weitere Informationen finden Sie unter [„Java-Voraussetzungen für den Endpoint Operations Management-Agenten“](#), auf Seite 47.

Je nach verwendeter Umgebung und verwendetem Installationspaket müssen Sie den Speicherort der JRE für Ihre Agenten definieren. Folgende Umgebungen erfordern die Konfiguration des JRE-Speicherorts.

- Plattformspezifische Agenteninstallation auf einer Maschine, die eine eigene zu verwendende JRE hat
- Plattformunabhängige Agenteninstallation

So löst der Agent seine JRE auf

Der Agent löst seine JRE basierend auf dem Plattformtyp auf.

UNIX-Plattformen

Auf UNIX-Plattformen bestimmt der Agent in dieser Reihenfolge, welche JRE verwendet wird:

- 1 HQ_JAVA_HOME-Umgebungsvariable
- 2 Integrierte JRE
- 3 JAVA_HOME-Umgebungsvariable

Linux-Plattformen

Auf Linux-Plattformen können Sie `export HQ_JAVA_HOME= path_to_current_java_directory` verwenden, um eine Systemvariable zu definieren.

Windows-Plattformen

Auf Windows-Plattformen löst der Agent die zu verwendende JRE in dieser Reihenfolge auf:

- 1 HQ_JAVA_HOME-Umgebungsvariable

Der Pfad, der in der Variable definiert ist, darf keine Leerzeichen enthalten. Verwenden Sie eventuell eine verkürzte Version des Pfades, indem Sie eine Tilde (~) einfügen. So wird beispielsweise `c:\Program Files\Java\jre7` zu `c:\Progra~1\Java\jre7`. Die Zahl nach der Tilde ist abhängig von der alphabetischen Reihenfolge (wobei a = 1, b = 2 und so weiter) der Dateien, deren Name mit `progra` in diesem Verzeichnis beginnt.

- 2 Integrierte JRE

Sie definieren eine Systemvariable über das Menü **Mein Computer**. Wählen Sie **Eigenschaften > Erweitert > Umgebungsvariablen > Systemvariablen > Neu**.

Aufgrund eines unbekannten Problems mit Windows können Windows-Dienste auf Windows Server 2008 R2 und 2012 R2 alte Werte der Systemvariablen speichern, obwohl diese aktualisiert oder entfernt wurden. Als Folge davon werden Aktualisierungen oder das Entfernen der HQ_JAVA_HOME-Systemvariable unter Umständen nicht an den Endpoint Operations Management-Agentenservice übergeben. In diesem Fall kann der Endpoint Operations Management-Agent einen veralteten Wert für HQ_JAVA_HOME verwenden, der dazu führt, dass die falsche JRE-Version verwendet wird.

Systemvoraussetzungen für den Endpoint Operations Management -Agenten

Wenn Sie `localhost` nicht als Loopback-Adresse festlegen, wird der Endpoint Operations Management-Agent nicht registriert, und der folgende Fehler tritt auf: `Verbindung fehlgeschlagen. Server heruntergefahren (oder falsche/r IP-Adresse/Port verwendet)`. Warten Sie 10 Sekunden, bevor Sie es erneut versuchen.

Als Abhilfe führen Sie die folgenden Schritte aus:

Vorgehensweise

- 1 Öffnen Sie die Hosts-Datei `/etc/hosts` unter Linux bzw. `C:\Windows\System32\Drivers\etc\hosts` unter Windows.
- 2 Ändern Sie die Datei so, dass sie eine `localhost`-Zuordnung zur IPv4-Loopback-Adresse `127.0.0.1` aufweist, verwenden Sie dazu `127.0.0.1 localhost`.
- 3 Speichern Sie die Datei.

Endpoint Operations Management-Agent unterstützt nicht IPv6.

Konfigurieren des Endpoint Operations Management -Agenten mit vRealize Operations Manager -Server-Kommunikationseigenschaften

Vor dem ersten Starten des Agenten können Sie in der Datei `agent.properties` die Eigenschaften, die dem Agenten die Kommunikation mit dem vRealize Operations Manager-Server ermöglichen, sowie weitere Agenteneigenschaften definieren. Wenn Sie den Agenten in der Eigenschaftsdatei konfigurieren, können Sie die Bereitstellung für mehrere Agenten optimieren.

Wenn eine Eigenschaftsdatei vorhanden ist, sichern Sie sie, bevor Sie Änderungen an der Konfiguration vornehmen. Wenn der Agent keine Eigenschaftsdatei hat, erstellen Sie eine.

Ein Agent sucht in `AgentHome/conf` nach seiner Eigenschaftsdatei. Dies ist der Standardspeicherort für `agent.properties`.

Wenn der Agent die erforderlichen Eigenschaften für die Herstellung der Kommunikation mit dem vRealize Operations Manager-Server an einem dieser Speicherorte nicht findet, fordert er beim ersten Starten des Agenten zur Eingabe der Eigenschaftenwerte auf.

Es sind mehrere Schritte erforderlich, um die Konfiguration abzuschließen.

Sie können vor oder nach dem ersten Starten einige Agenteneigenschaften definieren. Vor dem ersten Starten müssen immer Eigenschaften konfiguriert werden, die folgende Verhaltensweise steuern.

- Wenn der Agent einen SSL-Keystore, den Sie verwalten, anstelle eines von vRealize Operations Manager generierten Keystores verwenden soll.
- Wenn der Agent die Verbindung zum vRealize Operations Manager-Server über einen Proxyserver herstellen soll.

Voraussetzungen

Stellen Sie sicher, dass der vRealize Operations Manager-Server ausgeführt wird.

Vorgehensweise

- 1 [Endpoint Operations Management-Agenten-zu-vRealize Operations Manager-Server-Konfigurationseigenschaften aktivieren](#) auf Seite 50

In der Datei `agent.properties` sind Eigenschaften, die sich auf die Kommunikation zwischen dem Endpoint Operations Management-Agenten und dem vRealize Operations Manager-Server beziehen, standardmäßig deaktiviert. Sie müssen Sie aktivieren.

- 2 [Festlegen der Endpoint Operations Management-Agenten-Konfigurationseigenschaften](#) auf Seite 50
- Die Datei `agent.properties` enthält Eigenschaften, die Sie zum Verwalten der Kommunikation konfigurieren können.

- 3 [Konfigurieren eines Endpoint Operations Management-Agenten-Keystores](#) auf Seite 52

Der Agent verwendet für die interne Kommunikation ein selbstsigniertes Zertifikat und ein zweites Zertifikat, das während der Agentenregistrierung vom Server signiert wird. Standardmäßig werden die Zertifikate in einem Keystore gespeichert, der im Order `data` erstellt wird. Sie können Ihren eigenen Keystore für die Verwendung durch den Agenten konfigurieren.

- 4 [Konfigurieren des Endpoint Operations Management-Agenten mit dem Konfigurationsdialog](#) auf Seite 52

Der Dialog für die Endpoint Operations Management-Agentenkonfiguration wird in der Shell angezeigt, wenn Sie einen Agenten starten, der keine Konfigurationswerte aufweist, die den Speicherort des vRealize Operations Manager-Servers angeben. In diesem Dialog werden Sie aufgefordert, die Adresse und den Port des vRealize Operations Manager-Servers und andere Verbindungsdaten anzugeben.

- 5 [Überschreiben von Eigenschaften für die Konfiguration von Agenten](#) auf Seite 53
Sie können angeben, dass vRealize Operations Manager die Standardeigenschaften für Agenten überschreibt, wenn sie sich von den von Ihnen definierten benutzerdefinierten Eigenschaften unterscheiden.
- 6 [Endpoint Operations Management-Agenteneigenschaften](#) auf Seite 54
Mehrere Eigenschaften werden in der Datei `agent.properties` für einen Endpoint Operations Management-Agenten unterstützt. Nicht alle unterstützten Eigenschaften sind standardmäßig in der Datei `agent.properties` enthalten.

Weiter

Starten Sie den Endpoint Operations Management-Agent.

Endpoint Operations Management -Agenten-zu- vRealize Operations Manager -Server-Konfigurationseigenschaften aktivieren

In der Datei `agent.properties` sind Eigenschaften, die sich auf die Kommunikation zwischen dem Endpoint Operations Management-Agenten und dem vRealize Operations Manager-Server beziehen, standardmäßig deaktiviert. Sie müssen Sie aktivieren.

Vorgehensweise

- 1 Suchen Sie in der Datei `agent.properties` den folgenden Abschnitt.

```
## Use the following to automate agent setup
## using these properties.
##
## If any properties do not have values specified, the setup
## process prompts for their values.
##
## If the value to use during automatic setup is the default, use the string *default* as
the value for the option.
```

- 2 Entfernen Sie das Hashtag am Anfang jeder Zeile, um die Eigenschaften zu aktivieren.

```
#agent.setup.serverIP=localhost
#agent.setup.serverSSLPort=443
#agent.setup.serverLogin=username
#agent.setup.serverPword=password
```

Wenn Sie den Endpoint Operations Management-Agenten zum ersten Mal starten und `agent.setup.serverPword` inaktiv ist und einen Klartextwert hat, verschlüsselt der Agent den Wert.

- 3 (Optional) Entfernen Sie das Hashtag am Anfang der Zeile `#agent.setup.serverCertificateThumbprint=` und geben Sie einen Fingerabdruckwert an, um die Vorabgenehmigung des Serverzertifikats zu aktivieren.

Festlegen der Endpoint Operations Management -Agenten-Konfigurationseigenschaften

Die Datei `agent.properties` enthält Eigenschaften, die Sie zum Verwalten der Kommunikation konfigurieren können.

Die Konfiguration des Agentenservers erfordert einen Mindestsatz an Eigenschaften.

Vorgehensweise

- 1 Legen Sie den Speicherort und die Anmeldedaten fest, die der Agent verwenden muss, um den vRealize Operations Manager-Server zu kontaktieren.

Eigenschaft	Eigenschaftsdefinition
agent.setup.serverIP	Legen Sie die Adresse oder den Hostnamen des vRealize Operations Manager-Servers fest.
agent.setup.serverSSLPort	Der Standardwert ist der standardmäßige SSL-Listenerport des vRealize Operations Manager-Servers. Wenn Ihr Server für einen anderen Listenerport konfiguriert ist, geben Sie die Portnummer an.
agent.setup.serverLogin	Geben Sie den Benutzernamen für den Agenten an, der für die Kommunikation mit dem vRealize Operations Manager-Server verwendet werden soll. Wenn Sie den Standardwert für <code>username</code> ändern, prüfen Sie, ob das Benutzerkonto auf dem vRealize Operations Manager-Server korrekt konfiguriert ist.
agent.setup.serverPword	Legen Sie das Kennwort für den Agenten zusammen mit dem in <code>agent.setup.camLogin</code> festgelegten Benutzernamen fest, um die Verbindung zum vRealize Operations Manager-Server herzustellen. Prüfen Sie, ob das Kennwort das in vRealize Operations Manager für das Benutzerkonto konfigurierte ist.

- 2 (Optional) Geben Sie den Fingerabdruck des vRealize Operations Manager-Serverzertifikats an.

Eigenschaft	Eigenschaftsdefinition
agent.setup.serverCertificateThumbprint	<p>Liefert Details zum vertrauenswürdigen Serverzertifikat.</p> <p>Dieser Parameter ist erforderlich, um eine Installation ohne Benutzereingaben durchzuführen.</p> <p>Für den Fingerabdruck kann entweder der SHA1- oder der SHA256-Algorithmus verwendet werden.</p> <p>Standardmäßig generiert der vRealize Operations Manager-Server ein selbstsigniertes CA-Zertifikat, das zum Signieren des Zertifikats aller Knoten im Cluster verwendet wird. In diesem Fall muss der Fingerabdruck der des CA-Zertifikats sein, damit der Agent mit allen Knoten kommuniziert.</p> <p>Als vRealize Operations Manager-Administrator können Sie ein benutzerdefiniertes Zertifikat importieren, anstatt das standardmäßige zu verwenden. In diesem Fall müssen Sie als Wert für diese Eigenschaft einen Fingerabdruck festlegen, der diesem Zertifikat entspricht.</p> <p>Um den Wert des Zertifikatsfingerabdrucks einzusehen, loggen Sie sich in die vRealize Operations Manager-Verwaltungsschnittstelle unter <code>https://IP Address/admin</code> ein, und klicken Sie auf das SSL Zertifikat-Symbol rechts in der Menüleiste. Falls Sie das Originalzertifikat nicht durch ein angepasstes Zertifikat ersetzt haben, ist der zweite Fingerabdruck in der Liste der richtige. Falls Sie ein angepasstes Zertifikat hochgeladen haben, ist der erste Fingerabdruck in der Liste der richtige.</p>

- 3 (Optional) Legen Sie den Speicherort und den Dateinamen der Plattformtokendatei fest.

Diese Datei wird vom Agenten während der Installation erstellt und enthält den Identitätstoken für das Plattformobjekt.

Eigenschaft	Eigenschaftsdefinition
Windows: agent.setup.tokenFileWindows	Liefert Details über den Speicherort und den Dateinamen der Plattformtokendatei.
Linux: agent.setup.tokenFileLinux	<p>Der Wert darf keinen Backslash (\), kein Prozentzeichen (%) und keine Umgebungsvariablen enthalten.</p> <p>Verwenden Sie zum Angeben des Windows-Pfads Schrägstriche (/).</p>

- 4 (Optional) Spezifizieren Sie alle weiteren gewünschten Eigenschaften durch Ausführen des geeigneten Befehls.

Betriebssystem	Befehl
Linux	<code>./bin/ep-agent.sh set-property PropertyKey PropertyValue</code>
Windows	<code>./bin/ep-agent.bat set-property PropertyKey PropertyValue</code>

Die Eigenschaften sind in der `agent.properties`-Datei verschlüsselt.

Konfigurieren eines Endpoint Operations Management -Agenten-Keystores

Der Agent verwendet für die interne Kommunikation ein selbstsigniertes Zertifikat und ein zweites Zertifikat, das während der Agentenregistrierung vom Server signiert wird. Standardmäßig werden die Zertifikate in einem Keystore gespeichert, der im Order `data` erstellt wird. Sie können Ihren eigenen Keystore für die Verwendung durch den Agenten konfigurieren.

WICHTIG Um Ihren eigenen Keystore zu verwenden, müssen Sie diese Aktion vor der ersten Agentenaktivierung durchführen.

Vorgehensweise

- 1 Aktivieren Sie in der Datei `agent.properties` die Eigenschaften `# agent.keystore.path=` und `# agent.keystore.password=`.
Definieren Sie den vollständigen Pfad zum Keystore mit `agent.keystore.path` und das Keystore-Kennwort mit `agent.keystore.password`.
- 2 Fügen Sie die `[agent.keystore.alias]`-Eigenschaft zur Eigenschaftsdatei hinzu und legen Sie sie auf das Alias des primären Zertifikats oder den privaten Schlüsseleintrag des primären Keystore-Zertifikats fest.

Konfigurieren des Endpoint Operations Management -Agenten mit dem Konfigurationsdialog

Der Dialog für die Endpoint Operations Management-Agentenkonfiguration wird in der Shell angezeigt, wenn Sie einen Agenten starten, der keine Konfigurationswerte aufweist, die den Speicherort des vRealize Operations Manager-Servers angeben. In diesem Dialog werden Sie aufgefordert, die Adresse und den Port des vRealize Operations Manager-Servers und andere Verbindungsdaten anzugeben.

Der Dialog für die Agentenkonfiguration wird unter folgenden Umständen angezeigt:

- Wenn Sie einen Agenten zum ersten Mal starten und eine oder mehrere der relevanten Eigenschaften nicht in der Datei `agent.properties` angegeben haben.
- Wenn Sie einen Agenten starten, dessen gespeicherte Serververbindungsdaten beschädigt sind oder entfernt wurden.

Alternativ können Sie auch den Agenten-Launcher ausführen, um den Konfigurationsdialog zu öffnen.

Voraussetzungen

Stellen Sie sicher, dass der Server ausgeführt wird.

Vorgehensweise

- 1 Öffnen Sie ein Terminal-Fenster auf der Plattform, auf der der Agent installiert ist.
- 2 Navigieren Sie zum Verzeichnis `AgentHome/bin`.

- 3 Führen Sie den Agenten-Launcher mit der Start- oder Konfigurationsoption aus.

Plattform	Befehl
UNIX	<code>ep-agent.sh start</code>
Windows	<p>Installieren Sie den Windows-Service für den Agenten und führen Sie dann den Befehl <code>it: ep-agent.bat install ep-agent.bat start</code> aus.</p> <p>Wenn Sie einen Endpoint Operations Management-Agenten als einen Windows-Dienst konfigurieren, müssen Sie sicherstellen, dass die festgelegten Anmeldedaten ausreichen, damit sich der Dienst mit der Überwachungstechnologie verbinden kann. Wenn Sie beispielsweise einen Endpoint Operations Management-Agenten haben, der auf einem Microsoft SQL-Server läuft, und sich nur ein bestimmter Benutzer an diesem Server anmelden kann, muss die Anmeldung für den Windows-Dienst auch für diesen bestimmten Benutzer gelten.</p>

- 4 Reagieren Sie auf die Eingabeaufforderungen und beachten Sie dabei Folgendes.

Eingabeaufforderung	Beschreibung
Den Hostnamen oder die IP-Adresse des Servers eingeben	Wenn sich der Server auf derselben Maschine befindet wie der Agent, können Sie <code>localhost</code> eingeben. Wenn eine Firewall den Datenaustausch zwischen dem Agenten und dem Server blockiert, geben Sie die Adresse der Firewall an.
SSL-Port des Servers eingeben	Legen Sie den SSL-Port auf dem vRealize Operations Manager-Server fest, mit dem sich der Agent verbinden muss. Der Standardport lautet 443.
Der Server hat ein nicht vertrauenswürdiges Zertifikat ausgegeben	Wenn diese Warnung angezeigt wird, Ihr Server jedoch mit einem vertrauenswürdigen Zertifikat signiert wird, oder wenn Sie die <code>thumbprint</code> -Eigenschaft dahingehend aktualisiert haben, dass sie den Fingerabdruck enthält, könnte dieser Agent Opfer eines Man-in-the-Middle-Angriffs sein. Prüfen Sie die angezeigten Details des Zertifikatfingerabdrucks eingehend.
Serverbenutzername eingeben	Geben Sie den Namen eines vRealize Operations Manager-Benutzers mit <code>agentManager</code> -Berechtigungen ein.
Serverkennwort eingeben	Geben Sie das Kennwort für den festgelegten vRealize Operations Manager ein. Speichern Sie das Kennwort nicht in der Datei <code>agent.properties</code> .

Der Agent stellt eine Verbindung zum vRealize Operations Manager-Server her und der Server prüft, ob der Agent autorisiert ist, mit ihm zu kommunizieren.

Der Server generiert ein Client-Zertifikat, das den Agenten-Token enthält. Die Meldung `The agent has been successfully registered` wird angezeigt. Der Agent beginnt mit der Erkennung der Plattform und der darauf laufenden Produkte.

Überschreiben von Eigenschaften für die Konfiguration von Agenten

Sie können angeben, dass vRealize Operations Manager die Standardeigenschaften für Agenten überschreibt, wenn sie sich von den von Ihnen definierten benutzerdefinierten Eigenschaften unterscheiden.

Wenn Sie im Abschnitt „Erweitert“ im Dialogfeld „Objekt bearbeiten“ für **Konfigurationsdaten für Agenten überschreiben falsch** festlegen, werden die Standardkonfigurationsdaten für den Agenten angewendet. Wenn Sie für **Konfigurationsdaten für Agenten überschreiben wahr** festlegen, werden die Standardparameterwerte für Agenten ignoriert, wenn Sie alternative Werte festgelegt haben. Dabei werden die von Ihnen festgelegten Werte angewendet.

Wenn Sie den Wert **Agentenkonfigurationsdaten überschreiben** beim Bearbeiten eines MSSQL-Objekts (MSSQL, MSSQL-Datenbank, MSSQL-Berichtservices, MSSQL-Analyseservices oder MSSQL-Agent), das in einem Cluster ausgeführt wird, auf **wahr** setzen, kann dies zu inkonsistentem Verhalten führen.

Endpoint Operations Management -Agenteneigenschaften

Mehrere Eigenschaften werden in der Datei `agent.properties` für einen Endpoint Operations Management-Agenten unterstützt. Nicht alle unterstützten Eigenschaften sind standardmäßig in der Datei `agent.properties` enthalten.

Sie müssen alle Eigenschaften hinzufügen, die Sie verwenden möchten, die jedoch nicht in der `agent.properties`-Standarddatei enthalten sind.

Sie können Eigenschaften in der Datei `agent.properties` verschlüsseln, um die unbeaufsichtigte Installation zu ermöglichen.

Verschlüsseln von Eigenschaftswerten des Endpoint Operations Management -Agenten

Nach der Installation eines Endpoint Operations Management-Agenten können Sie damit verschlüsselte Werte der Datei `agent.properties` hinzufügen, um eine unbeaufsichtigte Installation zu ermöglichen.

Wenn Sie z. B. ein Benutzerkennwort angeben möchten, rufen Sie `./bin/ep-agent.sh set-property agent.setup.serverPword serverPasswordValue` auf, um die folgende Zeile der Datei `agent.properties` hinzuzufügen.

```
agent.setup.serverPword = ENC(4FyUf6m/c5i+RriaNpSEQ1WKGb4y+Dhp7213XQiyvtwI4tM1bGJfZMBPG23KnsU-
Wu30KrW35gB+Ms20snM4TDg==)
```

Der zur Verschlüsselung des Werts verwendete Schlüssel wird in `AgentHome/conf/agent.scu` gespeichert. Wenn Sie andere Werte verschlüsseln, wird dazu der zur Verschlüsselung des ersten Werts verwendete Schlüssel genutzt.

Voraussetzungen

Vergewissern Sie sich, dass der Endpoint Operations Management-Agent auf `AgentHome/conf/agent.scu` zugreifen kann. Nach der Verschlüsselung der Agent-Server-Verbindungseigenschaften kann der Agent nur gestartet werden, wenn der Zugriff auf diese Datei möglich ist.

Vorgehensweise

- ◆ Öffnen Sie eine Befehlseingabeaufforderung und führen Sie `./bin/ep-agent.sh set-property agent.setup.propertyName propertyValue` aus.

Der zur Verschlüsselung des Werts verwendete Schlüssel wird in `AgentHome/conf/agent.scu` gespeichert.

Weiter

Wenn Ihre Bereitstellungsstrategie für Agenten die Verteilung einer `agent.properties`-Standarddatei an alle Agenten umfasst, müssen Sie ebenfalls `agent.scu` verteilen. Weitere Informationen hierzu finden Sie unter „[Gleichzeitiges Installieren mehrerer Endpoint Operations Management-Agenten](#)“, auf Seite 75.

Hinzufügen von Eigenschaften zur Datei agent.properties

Sie müssen alle Eigenschaften, die verwendet werden sollen und die nicht in der standardmäßigen Datei `agent.properties` enthalten sind, hinzufügen.

Im Folgenden finden Sie eine Liste der verfügbaren Eigenschaften.

- [agent.keystore.alias-Eigenschaft](#) auf Seite 57
Diese Eigenschaft konfiguriert den Namen des benutzerverwalteten Keystores für den Agenten, wenn Agenten für unidirektionale Kommunikation mit dem vRealize Operations Manager-Server konfiguriert wurden.
- [agent.keystore.password-Eigenschaft](#) auf Seite 58
Diese Eigenschaft konfiguriert das Passwort für den SSL-Keystore eines Endpoint Operations Management-Agenten.

- [agent.keystore.path-Eigenschaft](#) auf Seite 58
Diese Eigenschaft konfiguriert den Speicherort des SSL-Keystore eines Endpoint Operations Management-Agenten.
- [agent.listenPort-Eigenschaft](#) auf Seite 58
Diese Eigenschaft legt den Port fest, auf dem der Endpoint Operations Management-Agent hört, um die Kommunikation vom vRealize Operations Manager-Server zu empfangen.
- [agent.logDir-Eigenschaft](#) auf Seite 59
Sie können diese Eigenschaft zur Datei `agent.properties` hinzufügen, um das Verzeichnis anzugeben, in die der Endpoint Operations Management-Agent seine Protokolldatei schreibt. Wenn Sie keinen vollständig qualifizierten Pfad angeben, wird `agent.logDir` relativ zum Agenteninstallationsverzeichnis bewertet.
- [agent.logFile-Eigenschaft](#) auf Seite 59
Der Pfad und der Name der Agentenprotokolldatei.
- [agent.logLevel Property](#) auf Seite 59
Der Detailgrad der Nachrichten, die der Agent in die Protokolldatei schreibt.
- [agent.logLevel.SystemErr-Eigenschaft](#) auf Seite 59
Leitet `System.err` zur Datei `agent.log` weiter.
- [agent.logLevel.SystemOut-Eigenschaft](#) auf Seite 59
Leitet `System.out` zur Datei `agent.log` weiter.
- [agent.proxyHost-Eigenschaft](#) auf Seite 60
Der Hostname oder die IP-Adresse des Proxyservers, zu dem der Endpoint Operations Management-Agent zuerst eine Verbindung herstellen muss, wenn er eine Verbindung zum vRealize Operations Manager-Server herstellt.
- [agent.proxyPort-Eigenschaft](#) auf Seite 60
Die Portnummer des Proxyservers, zu dem der Endpoint Operations Management-Agent zuerst eine Verbindung herstellen muss, wenn er eine Verbindung zum vRealize Operations Manager-Server herstellt.
- [agent.setup.acceptUnverifiedCertificate-Eigenschaft](#) auf Seite 60
Diese Eigenschaft steuert, ob ein Endpoint Operations Management-Agent eine Warnung ausgibt, wenn der vRealize Operations Manager-Server ein SSL-Zertifikat präsentiert, das sich nicht im Keystore des Agenten befindet und entweder selbstsigniert oder von einer anderen Zertifikatautorität signiert ist als derjenigen, die das SSL-Zertifikat des Agenten signiert hat.
- [agent.setup.camIP-Eigenschaft](#) auf Seite 60
Verwenden Sie diese Eigenschaft, um die IP-Adresse des vRealize Operations Manager-Servers für den Agenten zu definieren. Der Endpoint Operations Management-Agent liest diesen Wert nur, wenn er in seinem Datenverzeichnis keine Verbindungskonfiguration finden kann.
- [agent.setup.camLogin-Eigenschaft](#) auf Seite 61
Verwenden Sie beim ersten Start nach der Installation diese Eigenschaft, um den Benutzernamen des Endpoint Operations Management-Agenten zu definieren, der verwendet werden soll, wenn sich der Agent am Server registriert.
- [agent.setup.camPort-Eigenschaft](#) auf Seite 61
Verwenden Sie beim ersten Start nach der Installation diese Eigenschaft, um den Serverport des Endpoint Operations Management-Agenten zu definieren, der für nicht sichere Kommunikationen mit dem Server verwendet werden soll.

- [agent.setup.camPword-Eigenschaft](#) auf Seite 61
Verwenden Sie diese Eigenschaft, um das Passwort zu definieren, das der Endpoint Operations Management-Agent verwendet, wenn er eine Verbindung zum vRealize Operations Manager-Server herstellt, sodass der Agent einen Benutzer nicht auffordert, das Passwort bei der ersten Einrichtung interaktiv bereitzustellen.
- [agent.setup.camSecure](#) auf Seite 62
Diese Eigenschaft wird verwendet, wenn Sie Endpoint Operations Management am vRealize Operations Manager-Server registrieren, um mit Verschlüsselung zu kommunizieren.
- [agent.setup.camSSLPort-Eigenschaft](#) auf Seite 62
Verwenden Sie beim ersten Start nach der Installation diese Eigenschaft, um den Serverport des Endpoint Operations Management-Agenten zu definieren, der für SSL-Kommunikationen mit dem Server verwendet werden soll.
- [agent.setup.resetupToken-Eigenschaft](#) auf Seite 62
Verwenden Sie diese Eigenschaft, um einen Endpoint Operations Management-Agenten so zu konfigurieren, dass ein neuer Token erstellt wird, der für die Authentifizierung am Server beim Start verwendet wird. Das Regenerieren eines Tokens ist hilfreich, wenn der Agent keine Verbindung zum Server herstellen kann, weil der Token gelöscht wurde oder beschädigt ist.
- [agent.setup.unidirectional-Eigenschaft](#) auf Seite 62
Aktiviert unidirektionale Kommunikation zwischen dem Endpoint Operations Management-Agenten und dem vRealize Operations Manager-Server.
- [agent.startupTimeOut-Eigenschaft](#) auf Seite 62
Die Anzahl der Sekunden, die das Startup-Skript des Endpoint Operations Management-Agenten wartet, bis festgelegt wird, dass der Agent nicht erfolgreich gestartet ist. Wenn innerhalb dieses Zeitraums festgestellt wird, dass der Agent nicht auf Anfragen hört, wird ein Fehler protokolliert und es tritt eine Zeitüberschreitung des Startup-Skripts auf.
- [autoinventory.defaultScan.interval.millis-Eigenschaft](#) auf Seite 63
Legt fest, wie häufig der Endpoint Operations Management-Agent einen standardmäßigen, automatischen Bestandslistenscan durchführt.
- [autoinventory.runtimeScan.interval.millis-Eigenschaft](#) auf Seite 63
Legt fest, wie häufig ein Endpoint Operations Management-Agent einen Runtime-Scan durchführt.
- [http.useragent-Eigenschaft](#) auf Seite 63
Definiert den Wert für den User-Agent-Request-Header in HTTP-Anfrage, die vom Endpoint Operations Management-Agenten ausgegeben werden.
- [log4j-Eigenschaften](#) auf Seite 63
Hier werden die log4j-Eigenschaften für den Endpoint Operations Management-Agenten beschrieben.
- [platform.log_track.eventfmt-Eigenschaft](#) auf Seite 64
Gibt den Inhalt und das Format der Windows-Ereignisattribute an, die ein Endpoint Operations Management-Agent bei der Protokollierung eines Windows-Ereignisses als Ereignis in vRealize Operations Manager umfasst.
- [plugins.exclude-Eigenschaft](#) auf Seite 65
Legt die Plug-Ins fest, die der Endpoint Operations Management-Agent während des Startvorgangs nicht lädt. Dies ist hilfreich, um den Speicherbedarf des Agenten zu verringern.
- [plugins.include-Eigenschaft](#) auf Seite 66
Legt die Plug-Ins fest, die der Endpoint Operations Management-Agent während des Startvorgangs lädt. Dies ist hilfreich, um den Speicherbedarf des Agenten zu verringern.

- [postgresql.database.name.format Property](#) auf Seite 66
Diese Eigenschaft spezifiziert das Namensformat, das das PostgreSQL Plug-in automatisch erkannten PostgreSQL Database und vPostgreSQL Database Datenbanktypen zuweist.
- [postgresql.index.name.format Property](#) auf Seite 66
Diese Eigenschaft spezifiziert das Namensformat, das das PostgreSQL Plug-in automatisch erkannten PostgreSQL Index und vPostgreSQL Index Indextypen zuweist.
- [postgresql.server.name.format Property](#) auf Seite 67
Diese Eigenschaft spezifiziert das Namensformat, das das PostgreSQL Plug-in automatisch erkannten PostgreSQL und vPostgreSQL Servertypen zuweist.
- [postgresql.table.name.format Property](#) auf Seite 67
Diese Eigenschaft spezifiziert das Namensformat, das das PostgreSQL Plug-in automatisch erkannten PostgreSQL Table und vPostgreSQL Table Tabellentypen zuweist.
- [scheduleThread.cancelTimeout Property](#) auf Seite 68
Diese Eigenschaft spezifiziert die Maximalzeit in Millisekunden, die der ScheduleThread einen metrischen Erfassungsprozess zulässt, bevor ein Abbruchversuch gestartet wird.
- [scheduleThread.fetchLogTimeout Property](#) auf Seite 68
Diese Eigenschaft steuert, wann im Falle eines lang andauernden metrischen Erfassungsprozesses eine Warnmeldung ausgegeben wird.
- [scheduleThread.poolsize Property](#) auf Seite 68
Diese Eigenschaft ermöglicht es einem Plug-in, mehrere Threads für die Erfassung von Metriken zu verwenden. Die Eigenschaft kann den metrischen Durchsatz bei Plug-ins erhöhen, die bekanntermaßen thread-sicher sind.
- [scheduleThread.queueSize Property](#) auf Seite 69
Verwenden Sie die Eigenschaft, um die Warteschlange für die Erfassung von Metriken (Anzahl der Metriken) bei einem Plug-in zu begrenzen.
- [sigar.mirror.procnet Property](#) auf Seite 69
mirror /proc/net/tcp unter Linux.
- [sigar.pdh.enableTranslation-Eigenschaft](#) auf Seite 69
Verwenden Sie diese Eigenschaft, um die Übersetzung basierend auf der erkannten Sprachumgebung des Betriebssystems zu aktivieren.
- [snmpTrapReceiver.listenAddress Property](#) auf Seite 69
Spezifiziert den Port, über den der Endpoint Operations Management-Agent nach SNMP-Traps lauscht.

agent.keystore.alias-Eigenschaft

Diese Eigenschaft konfiguriert den Namen des benutzerverwalteten Keystores für den Agenten, wenn Agenten für unidirektionale Kommunikation mit dem vRealize Operations Manager-Server konfiguriert wurden.

Beispiel: Definieren des Namens eines Keystores

Bei diesem benutzerverwalteten Keystore für einen unidirektionalen Agenten

```
hq self-signed cert), Jul 27, 2011, trustedCertEntry,
Certificate fingerprint (MD5): 98:FF:B8:3D:25:74:23:68:6A:CB:0B:9C:20:88:74:CE
hq-agent, Jul 27, 2011, PrivateKeyEntry,
Certificate fingerprint (MD5): 03:09:C4:BC:20:9E:9A:32:DC:B2:E8:29:C0:3C:FE:38
```

definieren Sie den Namen des Keystores wie folgt:

```
agent.keystore.alias=hq-agent
```

Wenn der Wert dieser Eigenschaft nicht mit dem Keystore-Namen übereinstimmt, schlägt die Agent-Server-Kommunikation fehl.

Standard

Der Agent sucht standardmäßig nach dem hq-Keystore.

Für unidirektionale Agenten mit benutzerverwalteten Keystores müssen Sie den Keystore-Namen mithilfe dieser Eigenschaft definieren.

agent.keystore.password-Eigenschaft

Diese Eigenschaft konfiguriert das Passwort für den SSL-Keystore eines Endpoint Operations Management-Agenten.

Definieren Sie den Speicherort des Keystores mithilfe der „[agent.keystore.path-Eigenschaft](#)“, auf Seite 58-Eigenschaft.

Wenn Sie den Endpoint Operations Management-Agenten nach der Installation zum ersten Mal starten und `agent.keystore.password` nicht kommentiert ist und einen Klartextwert hat, verschlüsselt der Agent den Eigenschaftswert standardmäßig automatisch. Sie können diesen Eigenschaftswert vor dem Starten des Agenten selbst verschlüsseln.

Es empfiehlt sich, dasselbe Passwort für den Agenten-Keystore wie für den Privatschlüssel des Agenten zu verwenden.

Standard

Diese Eigenschaft ist in der Datei `agent.properties` standardmäßig nicht enthalten.

agent.keystore.path-Eigenschaft

Diese Eigenschaft konfiguriert den Speicherort des SSL-Keystore eines Endpoint Operations Management-Agenten.

Geben Sie den vollständigen Pfad zum Keystore an. Definieren Sie das Passwort für den Keystore mithilfe der `agent.keystore.password`-Eigenschaft. Weitere Informationen hierzu finden Sie unter „[agent.keystore.password-Eigenschaft](#)“, auf Seite 58.

Festlegen des Keystore-Pfads in Windows

Legen Sie den Pfad zum Keystore auf Windows-Plattformen in diesem Format fest.

```
C:/Documents and Settings/Desktop/keystore
```

Standard

```
AgentHome/data/keystore.
```

agent.listenPort-Eigenschaft

Diese Eigenschaft legt den Port fest, auf dem der Endpoint Operations Management-Agent hört, um die Kommunikation vom vRealize Operations Manager-Server zu empfangen.

Die Eigenschaft ist für unidirektionale Kommunikation nicht erforderlich.

agent.logDir-Eigenschaft

Sie können diese Eigenschaft zur Datei `agent.properties` hinzufügen, um das Verzeichnis anzugeben, in die der Endpoint Operations Management-Agent seine Protokolldatei schreibt. Wenn Sie keinen vollständig qualifizierten Pfad angeben, wird `agent.logDir` relativ zum Agenteninstallationsverzeichnis bewertet.

Um den Speicherort für die Agentenprotokolldatei zu ändern, geben Sie einen Pfad relativ zum Agenteninstallationsverzeichnis oder einen vollständig qualifizierten Pfad ein.

Beachten Sie, dass der Name der Agentenprotokolldatei mit der `agent.logFile`-Eigenschaft konfiguriert wird.

Standard

Diese Eigenschaft ist in der Datei `agent.properties` standardmäßig nicht enthalten.

Das Standardverhalten ist `agent.logDir=log`, was dazu führt, dass die Agentenprotokolldatei in das Verzeichnis `AgentHome/log` geschrieben wird.

agent.logFile-Eigenschaft

Der Pfad und der Name der Agentenprotokolldatei.

Standard

In der Datei `agent.properties` besteht die Standardeinstellung für die `agent.LogFile`-Eigenschaft aus einer Variable und einer Zeichenfolge,

```
agent.logFile=${agent.logDir}\agent.log
```

wo

- *agent.logDir* eine Variable ist, die den Wert einer identisch benannten Agenteneigenschaft bereitstellt. Standardmäßig ist der Wert von *agent.logDir* `log`, relativ zum Agenteninstallationsverzeichnis interpretiert.
- `agent.log` ist der Name der Agentenprotokolldatei.

Die Agentenprotokolldatei wird standardmäßig als `agent.log` benannt und in das Verzeichnis `AgentHome/log` geschrieben.

agent.logLevel Property

Der Detailgrad der Nachrichten, die der Agent in die Protokolldatei schreibt.

Zulässige Werte sind `INFO` und `DEBUG`.

Standard

`INFO`

agent.logLevel.SystemErr-Eigenschaft

Leitet `System.err` zur Datei `agent.log` weiter.

Das Auskommentieren dieser Einstellung führt dazu, dass `System.err` zu `agent.log.startup` weitergeleitet wird.

Standard

`ERROR`

agent.logLevel.SystemOut-Eigenschaft

Leitet `System.out` zur Datei `agent.log` weiter.

Das Auskommentieren dieser Einstellung führt dazu, dass `System.out` zu `agent.log.startup` weitergeleitet wird.

Standard

INFO

agent.proxyHost-Eigenschaft

Der Hostname oder die IP-Adresse des Proxyservers, zu dem der Endpoint Operations Management-Agent zuerst eine Verbindung herstellen muss, wenn er eine Verbindung zum vRealize Operations Manager-Server herstellt.

Diese Eigenschaft wird für Agenten unterstützt, die für unidirektionale Kommunikation konfiguriert sind.

Verwenden Sie diese Eigenschaft in Verbindung mit `agent.proxyPort` und `agent.setup.unidirectional`.

Standard

Keine

agent.proxyPort-Eigenschaft

Die Portnummer des Proxyservers, zu dem der Endpoint Operations Management-Agent zuerst eine Verbindung herstellen muss, wenn er eine Verbindung zum vRealize Operations Manager-Server herstellt.

Diese Eigenschaft wird für Agenten unterstützt, die für unidirektionale Kommunikation konfiguriert sind.

Verwenden Sie diese Eigenschaft in Verbindung mit `agent.proxyPort` und `agent.setup.unidirectional`.

Standard

Keine

agent.setup.acceptUnverifiedCertificate-Eigenschaft

Diese Eigenschaft steuert, ob ein Endpoint Operations Management-Agent eine Warnung ausgibt, wenn der vRealize Operations Manager-Server ein SSL-Zertifikat präsentiert, das sich nicht im Keystore des Agenten befindet und entweder selbstsigniert oder von einer anderen Zertifikatautorität signiert ist als derjenige, die das SSL-Zertifikat des Agenten signiert hat.

Wenn der Standard verwendet wird, gibt der Agent eine Warnung aus.

```
The authenticity of host 'localhost' can't be established.  
Are you sure you want to continue connecting? [default=no]:
```

Wenn Sie mit **Ja** antworten, importiert der Agent das Zertifikat des Servers und vertraut dem Zertifikat ab diesem Zeitpunkt.

Standard

```
agent.setup.acceptUnverifiedCertificate=no
```

agent.setup.camIP-Eigenschaft

Verwenden Sie diese Eigenschaft, um die IP-Adresse des vRealize Operations Manager-Servers für den Agenten zu definieren. Der Endpoint Operations Management-Agent liest diesen Wert nur, wenn er in seinem Datenverzeichnis keine Verbindungskonfiguration finden kann.

Sie können diese und andere `agent.setup.*`-Eigenschaften definieren, um die Benutzerinteraktion zu reduzieren, die zum Konfigurieren eines Agenten für die Kommunikation mit dem Server erforderlich ist.

Der Wert kann als IP-Adresse oder als vollständig qualifizierter Domänenname bereitgestellt werden. Um einen Server auf demselben Host zu identifizieren wie der Server, legen Sie den Wert auf 127.0.0.1 fest.

Wenn es eine Firewall zwischen dem Agenten und dem Server gibt, geben Sie die Adresse der Firewall an und konfigurieren Sie die Firewall so, dass Traffic an Port 7080, oder an 7443, wenn Sie den SSL-Port verwenden, an den vRealize Operations Manager-Server weitergeleitet wird.

Standard

Auskommentiert, localhost.

agent.setup.camLogin-Eigenschaft

Verwenden Sie beim ersten Start nach der Installation diese Eigenschaft, um den Benutzernamen des Endpoint Operations Management-Agenten zu definieren, der verwendet werden soll, wenn sich der Agent am Server registriert.

Die auf dem Server für diese Initialisierung erforderliche Berechtigung lautet Create für Plattformen.

Die Anmeldung des Agenten am Server ist nur während der ersten Konfiguration des Agenten erforderlich.

Der Agent liest diesen Wert nur, wenn er in seinem Datenverzeichnis keine Verbindungskonfiguration finden kann.

Sie können diese und andere `agent.setup.*`-Eigenschaften definieren, um die Benutzerinteraktion zu reduzieren, die zum Konfigurieren eines Agenten für die Kommunikation mit dem Server erforderlich ist.

Standard

Auskommentiert hqadmin.

agent.setup.camPort-Eigenschaft

Verwenden Sie beim ersten Start nach der Installation diese Eigenschaft, um den Serverport des Endpoint Operations Management-Agenten zu definieren, der für nicht sichere Kommunikationen mit dem Server verwendet werden soll.

Der Agent liest diesen Wert nur, wenn er in seinem Datenverzeichnis keine Verbindungskonfiguration finden kann.

Sie können diese und andere `agent.setup.*`-Eigenschaften definieren, um die Benutzerinteraktion zu reduzieren, die zum Konfigurieren eines Agenten für die Kommunikation mit dem Server erforderlich ist.

Standard

Auskommentiert 7080.

agent.setup.camPword-Eigenschaft

Verwenden Sie diese Eigenschaft, um das Passwort zu definieren, das der Endpoint Operations Management-Agent verwendet, wenn er eine Verbindung zum vRealize Operations Manager-Server herstellt, sodass der Agent einen Benutzer nicht auffordert, das Passwort bei der ersten Einrichtung interaktiv bereitzustellen.

Das Passwort für den Benutzer ist das von `agent.setup.camLogin` festgelegte.

Der Agent liest diesen Wert nur, wenn er in seinem Datenverzeichnis keine Verbindungskonfiguration finden kann.

Sie können diese und andere `agent.setup.*`-Eigenschaften definieren, um die Benutzerinteraktion zu reduzieren, die zum Konfigurieren eines Agenten für die Kommunikation mit dem Server erforderlich ist.

Wenn Sie den Endpoint Operations Management-Agenten nach der Installation zum ersten Mal starten und `agent.keystore.password` nicht kommentiert ist und einen Klartextwert hat, verschlüsselt der Agent den Eigenschaftswert automatisch. Sie können diese Eigenschaftswerte vor dem Starten des Agenten verschlüsseln.

Standard

Auskommentiert hqadmin.

agent.setup.camSecure

Diese Eigenschaft wird verwendet, wenn Sie Endpoint Operations Management am vRealize Operations Manager-Server registrieren, um mit Verschlüsselung zu kommunizieren.

Verwenden Sie `yes=secure`, `encrypted` oder `SSL` je nach Bedarf, um die Kommunikation zu verschlüsseln.

Verwenden Sie `no=unencrypted` für unverschlüsselte Kommunikation.

agent.setup.camSSLPort-Eigenschaft

Verwenden Sie beim ersten Start nach der Installation diese Eigenschaft, um den Serverport des Endpoint Operations Management-Agenten zu definieren, der für SSL-Kommunikationen mit dem Server verwendet werden soll.

Der Agent liest diesen Wert nur, wenn er in seinem Datenverzeichnis keine Verbindungskonfiguration finden kann.

Sie können diese und andere `agent.setup.*`-Eigenschaften definieren, um die Benutzerinteraktion zu reduzieren, die zum Konfigurieren eines Agenten für die Kommunikation mit dem Server erforderlich ist.

Standard

Auskommentiert 7443.

agent.setup.resetupToken-Eigenschaft

Verwenden Sie diese Eigenschaft, um einen Endpoint Operations Management-Agenten so zu konfigurieren, dass ein neuer Token erstellt wird, der für die Authentifizierung am Server beim Start verwendet wird. Das Regenerieren eines Tokens ist hilfreich, wenn der Agent keine Verbindung zum Server herstellen kann, weil der Token gelöscht wurde oder beschädigt ist.

Der Agent liest diesen Wert nur, wenn er in seinem Datenverzeichnis keine Verbindungskonfiguration finden kann.

Unabhängig vom Wert dieser Eigenschaft generiert ein Agent einen Token, wenn er nach der Installation zum ersten Mal gestartet wird.

Standard

Auskommentiert `no`.

agent.setup.unidirectional-Eigenschaft

Aktiviert unidirektionale Kommunikation zwischen dem Endpoint Operations Management-Agenten und dem vRealize Operations Manager-Server.

Wenn Sie einen Agenten für unidirektionale Kommunikation konfigurieren, wird jegliche Kommunikation mit dem Server vom Agenten initiiert.

Für einen unidirektionalen Agenten mit einem benutzerverwalteten Keystore müssen Sie den Keystore-Namen in der Datei `agent.properties` konfigurieren.

Standard

Auskommentiert `no`.

agent.startupTimeOut-Eigenschaft

Die Anzahl der Sekunden, die das Startup-Skript des Endpoint Operations Management-Agenten wartet, bis festgelegt wird, dass der Agent nicht erfolgreich gestartet ist. Wenn innerhalb dieses Zeitraums festgestellt wird, dass der Agent nicht auf Anfragen hört, wird ein Fehler protokolliert und es tritt eine Zeitüberschreitung des Startup-Skripts auf.

Standard

Diese Eigenschaft ist in der Datei `agent.properties` standardmäßig nicht enthalten.

Das Standardverhalten des Agenten ist eine Zeitüberschreitung nach 300 Sekunden.

autoinventory.defaultScan.interval.millis-Eigenschaft

Legt fest, wie häufig der Endpoint Operations Management-Agent einen standardmäßigen, automatischen Bestandslistenscan durchführt.

Der standardmäßige Scan erkennt Server- und Plattformdienstobjekte, normalerweise mithilfe der Prozess-tabelle oder der Windows-Registrierungsdatenbank. Standardmäßige Scans sind weniger ressourcenintensiv als Runtime-Scans.

Standard

Der Agent führt den standardmäßigen Scan beim Start und anschließend alle 15 Minuten durch.

Auskommentiert 86,400,000 Millisekunden oder ein Tag.

autoinventory.runtimeScan.interval.millis-Eigenschaft

Legt fest, wie häufig ein Endpoint Operations Management-Agent einen Runtime-Scan durchführt.

Ein Runtime-Scan verwendet unter anderem ressourcenintensivere Methoden zum Erkennen von Diensten als ein standardmäßiger Scan. So umfasst ein Runtime-Scan unter Umständen das Ausgeben einer SQL-Abfrage oder das Nachschlagen eines MBean.

Standard

86,400,000 Millisekunden oder ein Tag.

http.useragent-Eigenschaft

Definiert den Wert für den User-Agent-Request-Header in HTTP-Anfrage, die vom Endpoint Operations Management-Agenten ausgegeben werden.

Sie können mit `http.useragent` einen User-Agent-Wert definieren, der über Upgrades hinweg einheitlich ist.

Diese Eigenschaft ist in der Datei `agent.properties` standardmäßig nicht enthalten.

Standard

Standardmäßig fragt der User-Agent in Agent-Anfragen die Version des Endpoint Operations Management-Agenten ab, die sich bei einer Aktualisierung des Agenten ändert. Wenn ein Ziel-HTTP-Server so konfiguriert ist, dass Anfragen mit einem unbekannten User-Agent blockiert werden, schlagen Agent-Anfragen nach einer Aktualisierung des Agenten fehl.

Hyperic-HQ-Agent/Version, z. B. Hyperic-HQ-Agent/4.1.2-EE.

log4j-Eigenschaften

Hier werden die log4j-Eigenschaften für den Endpoint Operations Management-Agenten beschrieben.

```
log4j.rootLogger=${agent.logLevel}, R
```

```
log4j.appender.R.File=${agent.logFile}
```

```
log4j.appender.R.MaxBackupIndex=1
```

```
log4j.appender.R.MaxFileSize=5000KB
```

```
log4j.appender.R.layout.ConversionPattern=%d{dd-MM-yyyy HH:mm:ss,SSS} z} %-5p [%t] [%c{1}@%L] %m%n
```

```
log4j.appender.R.layout=org.apache.log4j.PatternLayout
```

```
log4j.appender.R=org.apache.log4j.RollingFileAppender
```

```
##
```

```
## Disable overly verbose logging
```

```
##
```

```

log4j.logger.org.apache.http=ERROR
log4j.logger.org.springframework.web.client.RestTemplate=ERROR
log4j.logger.org.hyperic.hq.measurement.agent.server.SenderThread=INFO
log4j.logger.org.hyperic.hq.agent.server.AgentDLListProvider=INFO
log4j.logger.org.hyperic.hq.agent.server.MeasurementSchedule=INFO
log4j.logger.org.hyperic.util.units=INFO
log4j.logger.org.hyperic.hq.product.pluginxml=INFO

# Only log errors from naming context
log4j.category.org.jnp.interfaces.NamingContext=ERROR
log4j.category.org.apache.axis=ERROR

#Agent Subsystems: Uncomment individual subsystems to see debug messages.
#-----
#log4j.logger.org.hyperic.hq.autoinventory=DEBUG
#log4j.logger.org.hyperic.hq.livedata=DEBUG
#log4j.logger.org.hyperic.hq.measurement=DEBUG
#log4j.logger.org.hyperic.hq.control=DEBUG

#Agent Plugin Implementations
#log4j.logger.org.hyperic.hq.product=DEBUG

#Server Communication
#log4j.logger.org.hyperic.hq.bizapp.client.AgentCallbackClient=DEBUG

#Server Realtime commands dispatcher
#log4j.logger.org.hyperic.hq.agent.server.CommandDispatcher=DEBUG

#Agent Configuration parser
#log4j.logger.org.hyperic.hq.agent.AgentConfig=DEBUG

#Agent plugins loader
#log4j.logger.org.hyperic.util.PluginLoader=DEBUG

#Agent Metrics Scheduler (Scheduling tasks definitions & executions)
#log4j.logger.org.hyperic.hq.agent.server.session.AgentSynchronizer.SchedulerThread=DEBUG

#Agent Plugin Managers
#log4j.logger.org.hyperic.hq.product.MeasurementPluginManager=DEBUG
#log4j.logger.org.hyperic.hq.product.AutoinventoryPluginManager=DEBUG
#log4j.logger.org.hyperic.hq.product.ConfigTrackPluginManager=DEBUG
#log4j.logger.org.hyperic.hq.product.LogTrackPluginManager=DEBUG
#log4j.logger.org.hyperic.hq.product.LiveDataPluginManager=DEBUG
#log4j.logger.org.hyperic.hq.product.ControlPluginManager=DEBUG

```

platform.log_track.eventfmt-Eigenschaft

Gibt den Inhalt und das Format der Windows-Ereignisattribute an, die ein Endpoint Operations Management-Agent bei der Protokollierung eines Windows-Ereignisses als Ereignis in vRealize Operations Manager umfasst.

Diese Eigenschaft ist in der Datei `agent.properties` standardmäßig nicht enthalten.

Standard

Bei der Aktivierung von Windows-Protokoll-Tracking wird ein Eintrag im Format [Timestamp] Log Message (EventLogName):EventLogName:EventAttributes bei Ereignissen protokolliert, die die Kriterien erfüllen, die Sie für die Ressource auf der Seite „Konfigurationseigenschaften“ festgelegt haben.

Attribut	Beschreibung
Timestamp	Zeitpunkt, als das Ereignis aufgetreten ist
Log Message	Eine Textzeichenfolge
EventLogName	Der Windows-Ereignisprotokolltyp System, Security oder Application
EventAttributes	Eine durch Doppelpunkt getrennte Zeichenfolge, die aus Quell- und Meldungsattributen des Windows-Ereignisses besteht

Beispielsweise wurde der Protokolleintrag: 04/19/2010 06:06 AM Log Message (SYSTEM): SYSTEM: Print: Printer HP LaserJet 6P was paused. für ein Windows-Ereignis geschrieben, das um 6:06 am 19.04.2010 in das Windows System-Ereignisprotokoll geschrieben wurde. Bei den Quell- und Meldungsattributen des Windows-Ereignisses handelt es sich um „Print“ und „Printer HP LaserJet 6P was paused.“.

Konfiguration

Mit den folgenden Parametern konfigurieren Sie die Windows-Ereignisattribute, die der Agent für ein Windows-Ereignis schreibt. Jeder Parameter entspricht einem Windows-Ereignisattribut mit demselben Namen.

Parameter	Beschreibung
%user%	Der Name des Benutzers, in dessen Namen das Ereignis aufgetreten ist.
%computer%	Der Name des Computers, auf dem das Ereignis aufgetreten ist.
%source%	Die Software, die das Windows-Ereignis protokolliert hat.
%event%	Ein Wert, durch den der bestimmte Ereignistyp identifiziert wird.
%message%	Die Ereignismeldung.
%category%	Ein anwendungsspezifischer Wert, der zur Gruppierung von Ereignissen verwendet wird.

Beispielsweise schreibt bei der Eigenschaftseinstellung `platform.log_track.eventfmt=%user%@%computer% %source%:%event%:%message%` der Endpoint Operations Management-Agent die folgenden Daten bei der Protokollierung des Windows-Ereignisses 04/19/2010 06:06 AM Log Message (SYSTEM): SYSTEM: HP_Administrator@Office Print:7:Printer HP LaserJet 6P was paused.. Dieser Eintrag wurde für ein Windows-Ereignis geschrieben, das um 6:06 am 19.04.2010 in das Windows System-Ereignisprotokoll geschrieben wurde. Die mit dem Ereignis verbundene Software wurde als „HP_Administrator“ auf dem Host „Office“ ausgeführt. Die Windows-Ereignis Quell-, Ereignis- und Meldungsattribute des Windows-Ereignisses lauten „Print“, „7“ und „Printer HP LaserJet 6P was paused“.

plugins.exclude-Eigenschaft

Legt die Plug-Ins fest, die der Endpoint Operations Management-Agent während des Startvorgangs nicht lädt. Dies ist hilfreich, um den Speicherbedarf des Agenten zu verringern.

Nutzung

Stellen Sie eine kommasetrennte Liste der auszuschließenden Plug-Ins bereit. Beispiel:

```
plugins.exclude=jboss,apache,mysql
```

plugins.include-Eigenschaft

Legt die Plug-Ins fest, die der Endpoint Operations Management-Agent während des Startvorgangs lädt. Dies ist hilfreich, um den Speicherbedarf des Agenten zu verringern.

Nutzung

Stellen Sie eine kommasetrennte Liste der einzuschließenden Plug-Ins bereit. Beispiel:

```
plugins.include=weblogic,apache
```

postgresql.database.name.format Property

Diese Eigenschaft spezifiziert das Namensformat, das das PostgreSQL Plug-in automatisch erkannten PostgreSQL Database und vPostgreSQL Database Datenbanktypen zuweist.

Standardmäßig ist der Name einer PostgreSQL oder vPostgreSQL Datenbank Database *DatabaseName*, wobei *DatabaseName* der automatisch erkannte Name für die Datenbank ist.

Definieren Sie `postgresql.database.name.format`, um eine andere Namenskonvention zu verwenden. Die von Ihnen verwendeten Bewegungsdaten müssen über das PostgreSQL Plug-in verfügbar sein.

Verwenden Sie folgende Syntax, um den standardmäßigen Tabellennamen, der vom Plug-in zugewiesen wurde, zu spezifizieren,

Database `${db}`

wobei

`postgresql.db` der automatisch erkannte Name der PostgreSQL oder vPostgreSQL Datenbank ist.

Standard

Diese Eigenschaft ist in der Datei `agent.properties` standardmäßig nicht enthalten.

postgresql.index.name.format Property

Diese Eigenschaft spezifiziert das Namensformat, das das PostgreSQL Plug-in automatisch erkannten PostgreSQL Index und vPostgreSQL Index Indextypen zuweist.

Standardmäßig ist der Name eines PostgreSQL oder vPostgreSQL Indexes Index *DatabaseName.Schema.Index*, in dem folgende Variablen enthalten sind

Variable	Beschreibung
DatabaseName	Automatisch erkannter Name der Datenbank.
Schema	Automatisch erkanntes Schema der Datenbank.
Index	Automatisch erkannter Name des Indexes.

Definieren Sie `postgresql.index.name.format`, um eine andere Namenskonvention zu verwenden. Die von Ihnen verwendeten Bewegungsdaten müssen über das PostgreSQL Plug-in verfügbar sein.

Verwenden Sie folgende Syntax, um den standardmäßigen Indexnamen, der vom Plug-in zugewiesen wurde, zu spezifizieren,

Index `${db}.${schema}.${index}`

wobei

Attribut	Beschreibung
db	Identifiziert die Hosting-Plattform des PostgreSQL oder vPostgreSQL Servers.
schema	Identifiziert das der Tabelle zugewiesene Schema.
index	Der Indexname in PostgreSQL.

Standard

Diese Eigenschaft ist in der Datei `agent.properties` standardmäßig nicht enthalten.

postgresql.server.name.format Property

Diese Eigenschaft spezifiziert das Namensformat, das das PostgreSQL Plug-in automatisch erkannten PostgreSQL und vPostgreSQL Servertypen zuweist.

Standardmäßig ist der Name eines PostgreSQL oder vPostgreSQL Servers *Host:Port*, in dem folgende Variablen enthalten sind

Variable	Beschreibung
Host	FQDN der Hosting-Plattform des Servers.
Port	Der PostgreSQL Listenerport.

Definieren Sie `postgresql.server.name.format`, um eine andere Namenskonvention zu verwenden. Die von Ihnen verwendeten Bewegungsdaten müssen über das PostgreSQL Plug-in verfügbar sein.

Verwenden Sie folgende Syntax, um den standardmäßigen Servernamen, der vom Plug-in zugewiesen wurde, zu spezifizieren,

```
${postgresql.host}:${postgresql.port}
```

wobei

Attribut	Beschreibung
postgresql.host	Identifiziert den FQDN der Hosting-Plattform.
postgresql.port	Identifiziert den Listener Port der Datenbank.

Standard

Diese Eigenschaft ist in der Datei `agent.properties` standardmäßig nicht enthalten.

postgresql.table.name.format Property

Diese Eigenschaft spezifiziert das Namensformat, das das PostgreSQL Plug-in automatisch erkannten PostgreSQL Table und vPostgreSQL Table Tabellentypen zuweist.

Standardmäßig ist der Name eines PostgreSQL oder vPostgreSQL Tabelle *Table DatabaseName.Schema.Table*, in dem folgende Variablen enthalten sind

Variable	Beschreibung
DatabaseName	Automatisch erkannter Name der Datenbank.
Schema	Automatisch erkanntes Schema der Datenbank.
Table	Automatisch erkannter Name der Tabelle.

Definieren Sie `postgresql.table.name.format`, um eine andere Namenskonvention zu verwenden. Die von Ihnen verwendeten Bewegungsdaten müssen über das PostgreSQL Plug-in verfügbar sein.

Verwenden Sie folgende Syntax, um den standardmäßigen Tabellennamen, der vom Plug-in zugewiesen wurde, zu spezifizieren,

```
Table ${db}.${schema}.${table}
```

wobei

Attribut	Beschreibung
<code>db</code>	die Hosting-Plattform des PostgreSQL oder vPostgreSQL Servers identifizieren.
<code>schema</code>	Identifiziert das der Tabelle zugewiesene Schema.
<code>table</code>	Der Tabellenname in PostgreSQL.

Standard

Diese Eigenschaft ist in der Datei `agent.properties` standardmäßig nicht enthalten.

scheduleThread.cancelTimeout Property

Diese Eigenschaft spezifiziert die Maximalzeit in Millisekunden, die der `ScheduleThread` einen metrischen Erfassungsprozess zulässt, bevor ein Abbruchversuch gestartet wird.

Erfolgt eine Zeitüberschreitung, wird die metrische Erfassungsprozess abgebrochen, wenn er sich in einem `wait()`, `sleep()` oder nicht blockierenden `read()` Status befindet.

Nutzung

```
scheduleThread.cancelTimeout=5000
```

Standard

5000 Millisekunden.

scheduleThread.fetchLogTimeout Property

Diese Eigenschaft steuert, wann im Falle eines lang andauernden metrischen Erfassungsprozesses eine Warnmeldung ausgegeben wird.

Übersteigt ein Prozess zur Erfassung von Metriken den Wert dieser Eigenschaft (gemessen in Millisekunden), schreibt der Agent eine Warnmeldung in die `agent-log` Datei.

Nutzung

```
scheduleThread.fetchLogTimeout=2000
```

Standard

2000 Millisekunden.

scheduleThread.poolsize Property

Diese Eigenschaft ermöglicht es einem Plug-in, mehrere Threads für die Erfassung von Metriken zu verwenden. Die Eigenschaft kann den metrischen Durchsatz bei Plug-ins erhöhen, die bekanntermaßen thread-sicher sind.

Nutzung

Spezifizieren Sie das Plug-in mittels Namen und Anzahl der Threads, um es der Erfassung von Metriken zuzuweisen

```
scheduleThread.poolsize.PluginName=2
```

wobei *PluginName* der Name des Plug-ins ist, dem Sie die Threads zuweisen. Beispiel:

```
scheduleThread.poolsize.vsphere=2
```

Standard

1

scheduleThread.queueSize Property

Verwenden Sie die Eigenschaft, um die Warteschlange für die Erfassung von Metriken (Anzahl der Metriken) bei einem Plug-in zu begrenzen.

Nutzung

Spezifizieren Sie das Plug-in durch den Namen und die maximale Länge der metrischen Warteschlange als Zahlenwert:

```
scheduleThread.queueSize.PluginName=15000
```

wobei *PluginName* der Name des Plug-ins ist, dem Sie die eine metrische Grenze auferlegen.

Beispiel:

```
scheduleThread.queueSize.vsphere=15000
```

Standard

1000

sigar.mirror.procnets Property

mirror /proc/net/tcp unter Linux.

Standard

true

sigar.pdh.enableTranslation-Eigenschaft

Verwenden Sie diese Eigenschaft, um die Übersetzung basierend auf der erkannten Sprachumgebung des Betriebssystems zu aktivieren.

snmpTrapReceiver.listenAddress Property

Spezifiziert den Port, über den der Endpoint Operations Management-Agent nach SNMP-Traps lauscht.

Diese Eigenschaft ist in der Datei `agent.properties` standardmäßig nicht enthalten.

SNMP verwendet üblicherweise den UDP Port 162 für Trap-Nachrichten. Dieser Port befindet sich im privilegierten Bereich, so dass ein Agent, der dort nach Trap-Nachrichten lauscht, als root oder als Administrator unter Windows laufen muss.

Sie können den Agenten auch als Nicht-Administrator einsetzen, indem Sie den Agenten so konfigurieren, dass er im nicht-privilegierten Bereich nach Trap-Nachrichten lauscht.

Nutzung

Geben Sie eine IP-Adresse an (oder 0.0.0.0, um alle Schnittstellen der Plattform zu spezifizieren) sowie einen Port für die UDP-Kommunikation im Format

```
snmpTrapReceiver.listenAddress=udp:IP_address/port
```

Um dem Endpoint Operations Management-Agenten zu ermöglichen, SNMP-Traps über einen nicht-privilegierten Port zu empfangen, wählen Sie Port 1024 oder größer. Die folgende Einstellung ermöglicht es dem Agenten, Traps über jede Schnittstelle der Plattform zu empfangen, über UDP-Port 1620.

```
snmpTrapReceiver.listenAddress=udp:0.0.0.0/1620
```

Verwalten der Agentenregistrierung auf vRealize Operations Manager -Servern

Die Endpoint Operations Management-Agenten identifizieren sich gegenüber dem Server mit Clientzertifikaten. Die Clientzertifikate werden durch den Agentenregistrierungsprozess generiert.

Das Clientzertifikat enthält einen Token, der als eindeutige Kennung verwendet wird. Wenn Sie vermuten, dass ein Client-Zertifikat gestohlen oder kompromittiert wurde, müssen Sie das Zertifikat ersetzen.

Sie benötigen AgentManager-Anmeldedaten, um den Agenten-Registrierungsprozess durchzuführen.

Wenn Sie einen Agenten entfernen oder neu installieren, indem Sie das Datenverzeichnis entfernen, wird der Agent Token beibehalten, um die Kontinuität der Daten zu ermöglichen. Weitere Informationen hierzu finden Sie unter [„Verstehen der Auswirkungen der Deinstallation und Neuinstallation von Agenten“](#), auf Seite 73.

Regenerieren des Clientzertifikats eines Agenten

Das Clientzertifikat eines Endpoint Operations Management-Agenten kann ablaufen und muss dann ersetzt werden. Sie würden z. B. ein Zertifikat ersetzen, das möglicherweise korrupt oder kompromittiert ist.

Voraussetzungen

Prüfen Sie, ob Sie über ausreichend Berechtigungen verfügen, um einen Endpoint Operations Management-Agenten bereitzustellen. Sie müssen vRealize Operations Manager-Benutzeranmeldeinformationen haben, die die Rolle umfassen, mit der Sie Endpoint Operations Management-Agenten installieren können. Weitere Informationen hierzu finden Sie unter [„Rollen und Berechtigungen in vRealize Operations Manager“](#), auf Seite 78.

Vorgehensweise

- ◆ Starten Sie den Registrierungsvorgang, indem Sie den Befehl `setup` für das Betriebssystem ausführen, auf dem der Agent läuft.

Betriebssystem	Befehl ausführen
Linux	<code>ep-agent.sh setup</code>
Windows	<code>ep-agent.bat setup</code>

Das Agenteninstallationsprogramm führt die Konfiguration aus, fordert ein neues Zertifikat vom Server an und importiert das neue Zertifikat in den Keystore.

Sichern der Kommunikation mit dem Server

Die Kommunikation von einem Endpoint Operations Management-Agenten zum vRealize Operations Manager-Server erfolgt nur in eine Richtung, aber beide Parteien müssen authentifiziert sein. Die Kommunikation wird immer mit TLS (Transport Layer Security) gesichert.

Wenn ein Agent nach der Installation zum ersten Mal eine Verbindung zum vRealize Operations Manager-Server initiiert, präsentiert der Server dem Agenten sein SSL-Zertifikat.

Wenn der Agent dem vom Server präsentierten Zertifikat vertraut, importiert der Agent das Zertifikat des Servers in seinen eigenen Keystore.

Der Agent vertraut einem Zertifikat, wenn dieses oder einer seiner Herausgeber (CA) bereits im Keystore des Agenten vorhanden ist.

Wenn der Agent dem vom Server präsentierten Zertifikat nicht vertraut, gibt der Agent standardmäßig eine Warnung aus. Sie können dem Zertifikat vertrauen oder den Konfigurationsvorgang abbrechen. Der vRealize Operations Manager-Server und der Agent importieren nicht vertrauenswürdige Zertifikate nur dann, wenn Sie die Warnung mit `yes` bestätigen.

Sie können den Agenten so konfigurieren, dass er einen bestimmten Fingerabdruck ohne Warnung akzeptiert, indem Sie den Fingerabdruck des Zertifikats für den vRealize Operations Manager-Server festlegen.

Standardmäßig generiert der vRealize Operations Manager-Server ein selbstsigniertes CA-Zertifikat, das zum Signieren des Zertifikats aller Knoten im Cluster verwendet wird. In diesem Fall muss der Fingerabdruck der des Herausgebers sein, damit der Agent mit allen Knoten kommuniziert.

Als vRealize Operations Manager-Administrator können Sie ein benutzerdefiniertes Zertifikat importieren, anstatt das standardmäßige zu verwenden. In diesem Fall müssen Sie als Wert für diese Eigenschaft einen Fingerabdruck festlegen, der diesem Zertifikat entspricht.

Für den Fingerabdruck kann entweder der SHA1- oder der SHA256-Algorithmus verwendet werden.

Starten von Agenten über eine Befehlszeile

Sie können Agenten über eine Befehlszeile aus den Betriebssystemen Linux und Windows starten.

Gehen Sie entsprechend den Vorgaben Ihres Betriebssystems vor.

Wenn Sie das Verzeichnis `data` löschen, verwenden Sie Windows Services nicht, um einen Endpoint Operations Management-Agenten anzuhalten und zu starten. Halten Sie den Agenten mit `epops-agent.bat stop` an. Löschen Sie das Verzeichnis `data`, und starten Sie den Agenten mit `epops-agent.bat start`.

Starten Sie den Agent Launcher von einer Linux Befehlszeile aus.

Sie können den Agent Launcher und Agent Lifecycle-Befehl mit dem `epops-agent.sh`-Skript in Verzeichnis `AgentHome/bin` ausführen.

Vorgehensweise

- 1 Öffnen Sie eine Eingabeaufforderung oder ein Terminalfenster.
- 2 Geben Sie den erforderlichen Befehl ein, indem Sie das Format `sh epops-agent.sh command`, wobei `command` eines der folgenden ist.

Option	Beschreibung
start	Startet den Agenten als Daemon-Prozess.
stop	Stoppt den JVM-Prozess des Agenten.
restart	Stoppt und startet nacheinander den JVM-Prozess des Agenten.
status	Frägt den Status des JVM-Prozesses des Agenten ab.
dump	Startet einen Thread-Dump für den Agenten-Prozess, und speichert das Ergebnis in der <code>agent.log</code> Datei unter <code>AgentHome/log</code> .
ping	Sendet einen Ping zum Agenten-Prozess
setup	Registriert das Zertifikat erneut mithilfe des bestehenden Tokens.

Starten Sie den Agent Launcher von einer Windows Befehlszeile aus.

Sie können den Agent Launcher und Agent Lifecycle-Befehl mit dem `epops-agent.bat`-Skript in Verzeichnis `AgentHome/bin` ausführen.

Vorgehensweise

- 1 Öffnen Sie ein Terminalfenster.
- 2 Geben Sie den erforderlichen Befehl ein, indem Sie das Format `epops-agent.bat command`, wobei `command` eines der folgenden ist.

Option	Beschreibung
install	Installieren Sie den NT-Dienst des Agenten. Führen Sie <code>start</code> aus, nachdem Sie <code>install</code> ausgeführt haben.
start	Startet den Agenten als NT-Dienst.
stop	Stoppt den Agenten als NT-Dienst.
remove	Entfernt den Dienst des Agenten aus der NT-Diensttabelle.
query	Frägt den derzeitigen Status des NT-Dienstes des Agenten ab (Status).

Option	Beschreibung
dump	Startet einen Thread-Dump für den Agenten-Prozess, und speichert das Ergebnis in der <code>agent.log</code> Datei unter <code>AgentHome/log</code> .
ping	Sendet einen Ping zum Agenten-Prozess
setup	Registriert das Zertifikat erneut mithilfe des bestehenden Tokens.

Verwalten eines Endpoint Operations Management -Agenten auf einer geklonten virtuellen Maschine

Wenn Sie eine virtuelle Maschine klonen, die einen Endpoint Operations Management-Agenten ausführt, der gerade Daten sammelt, müssen Sie bestimmte Prozesse durchführen, um Datenkontinuität zu gewährleisten.

Klonen einer virtuellen Maschine, um die ursprüngliche virtuelle Maschine zu löschen

Wenn Sie die virtuelle Maschine klonen, so dass Sie die ursprüngliche virtuelle Maschine löschen können, müssen Sie gewährleisten, dass die ursprüngliche virtuelle Maschine vom vCenter Server und aus dem vRealize Operations Manager gelöscht wird, so dass eine neue Beziehung zwischen Betriebssystem und virtueller Maschine angelegt werden kann.

Klonen einer virtuellen Maschine, um sie unabhängig von der ursprünglichen Maschine auszuführen

Wenn Sie eine virtuelle Maschine klonen, damit Sie beide Maschinen unabhängig von einander ausführen können, erfordert die geklonte Maschine einen neuen Agenten, weil ein Agent nur eine einzige Maschine überwachen kann.

Vorgehensweise

- ◆ Löschen Sie auf der geklonten Maschine den Endpoint Operations Management-Token und den Ordner `data` entsprechend dem Betriebssystem der Maschine.

Betriebssystem	Vorgang
Linux	Löschen Sie den Endpoint Operations Management-Token und den Ordner <code>data</code> .
Windows	<ol style="list-style-type: none"> 1 Führen Sie <code>epops-agent remove</code> aus. 2 Entfernen Sie den Agententoken und den Ordner <code>data</code>. 3 Führen Sie <code>epops-agent install</code> aus. 4 Führen Sie <code>epops-agent start</code> aus.

Verschieben von virtuellen Maschinen zwischen vCenter Server -Instanzen

Wenn Sie eine virtuelle Maschine von einem vCenter Server auf einen anderen verschieben, müssen Sie die ursprüngliche virtuelle Maschine von vRealize Operations Manager löschen, damit eine neue Betriebssystem-Beziehung mit der virtuellen Maschine angelegt werden kann.

Verstehen der Auswirkungen der Deinstallation und Neuinstallation von Agenten

Wenn Sie einen Endpoint Operations Management-Agenten deinstallieren und neu installieren, sind davon verschiedene Elemente betroffen, einschließlich bestehender Metriken, die der Agent gesammelt hat, und des Identifizierungstokens, der es einem neu installierten Agenten ermöglicht, die zuvor auf dem Server erkannten Objekte zu melden. Um Datenkontinuität zu gewährleisten, ist es wichtig, dass Sie sich der Auswirkungen der Deinstallation und Neuinstallation eines Agenten bewusst sind.

Es gibt zwei wichtige Speicherorte im Zusammenhang mit dem Agenten, die bei der Deinstallation beibehalten werden. Bevor Sie den Agenten deinstallieren, müssen Sie entscheiden, ob die Dateien beibehalten oder gelöscht werden sollen.

- Der Ordner `/data` wird während der Agenteninstallation erstellt. Er enthält den Keystore, sofern Sie für diesen keinen anderen Speicherort gewählt haben, und andere Daten im Zusammenhang mit dem aktuell installierten Agenten.
- Die Tokendatei der `epops-token`-Plattform wird vor der Agentenregistrierung erstellt und wird folgendermaßen gespeichert:
 - Linux: `/etc/vmware/epops-token`
 - Windows: `%PROGRAMDATA%/VMware/EP Ops Agent/epops-token`

Wenn Sie einen Agenten deinstallieren, müssen Sie den Ordner `/data` löschen. Das wirkt sich nicht auf die Datenkontinuität aus.

Um jedoch Datenkontinuität zu gewährleisten, ist es wichtig, dass Sie die Datei `epops-token` nicht löschen. Diese Datei enthält den Identitätstoken für das Plattformobjekt. Nach der Neuinstallation des Agenten ermöglicht dieser Token die Synchronisierung des Agenten mit den zuvor erkannten Objekten auf dem Server.

Wenn Sie den Agenten erneut installieren, informiert Sie das System darüber, ob es einen vorhandenen Token gefunden hat, und gibt seine Kennung an. Wenn ein Token gefunden wurde, verwendet das System diesen Token. Wenn kein Token gefunden wurde, erstellt das System einen neuen. Sollte ein Fehler auftreten, fordert Sie das System auf, entweder einen Speicherort und einen Dateinamen für die vorhandene Tokendatei oder einen Speicherort und einen Dateinamen für einen neuen anzugeben.

Die zum Deinstallieren eines Agenten verwendete Methode ist abhängig von der Installationsmethode.

- [Deinstallieren eines Agenten, der mit einem Archiv installiert wurde](#) auf Seite 74
Verwenden Sie diese Vorgehensweise, um Agenten zu deinstallieren, die Sie auf virtuellen Maschinen in Ihrer Umgebung mit einem Archiv installiert haben.
- [Deinstallieren eines Agenten, der mit einem RPM-Paket installiert wurde](#) auf Seite 74
Verwenden Sie diese Vorgehensweise, um Agenten zu deinstallieren, die Sie auf virtuellen Maschinen in Ihrer Umgebung mit einem RPM-Paket installiert haben.
- [Deinstallieren eines Agenten, der mit einer ausführbaren Windows-Datei installiert wurde](#) auf Seite 74
Verwenden Sie diese Vorgehensweise, um Agenten zu deinstallieren, die Sie auf virtuellen Maschinen in Ihrer Umgebung mit einer Windows EXE-Datei installiert haben.
- [Neuinstallieren eines Agenten](#) auf Seite 75
Wenn Sie die IP-Adresse, den Hostnamen oder die Portnummer des vRealize Operations Manager-Servers ändern, müssen Sie Ihre Agenten deinstallieren und erneut installieren.

Deinstallieren eines Agenten, der mit einem Archiv installiert wurde

Verwenden Sie diese Vorgehensweise, um Agenten zu deinstallieren, die Sie auf virtuellen Maschinen in Ihrer Umgebung mit einem Archiv installiert haben.

Voraussetzungen

Stellen Sie sicher, dass der Agent beendet wurde.

Vorgehensweise

- 1 (Optional) Führen Sie bei einem Windows-Betriebssystem `ep-agent.bat remove` aus, um den Agentenservice zu beenden.
- 2 Wählen Sie die geeignete Deinstallationsoption aus.
 - Wenn Sie den Agenten nach der Deinstallation nicht wieder installieren möchten, löschen Sie das Agentenverzeichnis.
Der Standardname des Verzeichnisses lautet `epops-agent-version`.
 - Wenn Sie den Agenten nach der Deinstallation erneut installieren möchten, löschen Sie das Verzeichnis `/data`.
- 3 (Optional) Wenn Sie nicht beabsichtigen, den Agenten nach der Deinstallation wieder zu installieren, oder wenn Sie die Datenintegrität nicht aufrechterhalten müssen, löschen Sie die Tokendatei der `epops-token`-Plattform.

Abhängig von Ihrem Betriebssystem ist die zu löschende Datei eine der folgenden, sofern in der Eigenschaftsdatei nicht anders angegeben.

- Linux: `/etc/epops/epops-token`
- Windows: `%PROGRAMDATA%/VMware/EP Ops Agent/epops-token`

Deinstallieren eines Agenten, der mit einem RPM-Paket installiert wurde

Verwenden Sie diese Vorgehensweise, um Agenten zu deinstallieren, die Sie auf virtuellen Maschinen in Ihrer Umgebung mit einem RPM-Paket installiert haben.

Wenn Sie einen Endpoint Operations Management Agenten deinstallieren, ist es sinnvoll, den Agenten zu beenden, um unnötige Belastungen des Servers zu verringern.

Vorgehensweise

- ◆ Öffnen Sie auf der virtuellen Maschine, von der Sie den Agenten entfernen, eine Befehlszeile und führen Sie `rpm -e epops-agent` aus.

Der Agent wird von der virtuellen Maschine deinstalliert.

Deinstallieren eines Agenten, der mit einer ausführbaren Windows-Datei installiert wurde

Verwenden Sie diese Vorgehensweise, um Agenten zu deinstallieren, die Sie auf virtuellen Maschinen in Ihrer Umgebung mit einer Windows EXE-Datei installiert haben.

Wenn Sie einen Endpoint Operations Management Agenten deinstallieren, ist es sinnvoll, den Agenten zu beenden, um unnötige Belastungen des Servers zu verringern.

Vorgehensweise

- ◆ Doppelklicken Sie im Installationszielverzeichnis für den Agenten auf `unins000.exe`.

Der Agent wird von der virtuellen Maschine deinstalliert.

Neuinstallieren eines Agenten

Wenn Sie die IP-Adresse, den Hostnamen oder die Portnummer des vRealize Operations Manager-Servers ändern, müssen Sie Ihre Agenten deinstallieren und erneut installieren.

Voraussetzungen

Um die Datenkontinuität zu wahren, müssen Sie beim Deinstallieren Ihres Agenten den `epops-token-PlatformToken` beibehalten. Weitere Informationen hierzu finden Sie unter „[Deinstallieren eines Agenten, der mit einem Archiv installiert wurde](#)“, auf Seite 74.

Wenn Sie einen Endpoint Operations Management-Agenten auf einer virtuellen Maschine neu installieren, werden bereits zuvor erkannte Objekte nicht mehr überwacht. Um diese Situation zu vermeiden, starten Sie den Endpoint Operations Management-Agenten erst, nachdem die Plug-In-Synchronisierung abgeschlossen ist.

Vorgehensweise

- ◆ Führen Sie den Agenteninstallationsvorgang für Ihr jeweiliges Betriebssystem aus.

Weitere Informationen hierzu finden Sie unter „[Auswählen eines Agenteninstallationspakets](#)“, auf Seite 40.

Weiter

Nachdem Sie einen Agenten installiert haben, empfangen MSSQL-Ressourcen möglicherweise keine Daten mehr. Wenn das der Fall ist, bearbeiten Sie die betreffenden Ressourcen und klicken Sie auf **OK**.

Gleichzeitiges Installieren mehrerer Endpoint Operations Management -Agenten

Wenn mehrere Endpoint Operations Management-Agenten gleichzeitig installiert werden sollen, können Sie eine standardisierte `agent.properties`-Datei erstellen, die von allen Agenten verwendet werden kann.

Für die Installation mehrerer Agenten sind eine Reihe von Schritten erforderlich. Führen Sie diese Schritte in der aufgeführten Reihenfolge aus.

Voraussetzungen

Prüfen Sie, ob die folgenden Voraussetzungen erfüllt werden.

- 1 Richten Sie einen Installationsserver ein.

Bei einem Installationsserver handelt es sich um einen Server, der auf die Zielplattformen zugreifen kann, von denen aus die Remote-Installation ausgeführt werden soll.

Der Server muss mit einem Benutzerkonto konfiguriert sein, das Berechtigungen für SSH für jede Zielplattform hat, ohne dass ein Kennwort erforderlich ist.

- 2 Prüfen Sie, ob jede Zielplattform, auf der ein Endpoint Operations Management-Agent installiert werden soll, folgende Elemente enthält.

- Ein Benutzerkonto, das mit dem auf dem Installationsserver erstellten identisch ist.
- Ein identisch benanntes Installationsverzeichnis, z. B. `/home/epomagent`.
- Ein vertrauenswürdiger Keystore, falls erforderlich.

Vorgehensweise

- 1 [Erstellen einer standardmäßigen Endpoint Operations Management-Agenteneigenschaftsdatei](#) auf Seite 76

Sie können eine Eigenschaftsdatei erstellen, die Eigenschaftswerte enthält, die von mehreren Agenten verwendet werden.

2 [Bereitstellen und Starten mehrerer Agenten nach einander](#) auf Seite 76

Sie können Remote-Installationen durchführen, um mehrere Agenten nach einander bereitzustellen, die eine einzelne Datei `agent.properties` verwenden.

3 [Bereitstellen und Starten mehrerer Agenten gleichzeitig](#) auf Seite 77

Sie können Remote-Installationen durchführen, um Agenten gleichzeitig bereitzustellen, die eine einzelne Datei `agent.properties` verwenden.

Erstellen einer standardmäßigen Endpoint Operations Management -Agenteneigenschaftsdatei

Sie können eine Eigenschaftsdatei erstellen, die Eigenschaftswerte enthält, die von mehreren Agenten verwendet werden.

Um die Bereitstellung mehrerer Agenten zu ermöglichen, erstellen Sie eine Datei `agent.properties`, die die erforderlichen Agenteneigenschaften enthält, damit der Agent starten und eine Verbindung mit dem vRealize Operations Manager-Server herstellen kann. Wenn Sie die erforderlichen Informationen in der Eigenschaftsdatei angegeben haben, lokalisiert jeder Agent beim Start seine Konfiguration und fordert Sie nicht auf, den Speicherort anzugeben. Sie können die Agenteneigenschaftsdatei in das Agenteninstallationsverzeichnis oder an einen Speicherort kopieren, der für den installierten Agenten verfügbar ist.

Voraussetzungen

Prüfen Sie, ob die Voraussetzungen in [„Gleichzeitiges Installieren mehrerer Endpoint Operations Management-Agenten“](#), auf Seite 75 erfüllt werden.

Vorgehensweise

1 Erstellen Sie eine Datei `agent.properties` in einem Verzeichnis.

Später kopieren Sie diese Datei auf andere Maschinen.

2 Konfigurieren Sie die Eigenschaften nach Bedarf.

Die Mindestkonfiguration enthält die IP-Adresse, den Benutzernamen, das Kennwort, den Fingerabdruck und den Port des vRealize Operations Manager-Installationsservers.

3 Speichern Sie Ihre Konfigurationen.

Wenn ein Agent zum ersten Mal gestartet wird, liest er die Datei `agent.properties`, um die Serververbindungsinformationen zu identifizieren. Die Agenten verbinden sich mit dem Server und registrieren sich.

Weiter

Führen Sie die Installation des Remote-Agenten durch. Siehe [„Bereitstellen und Starten mehrerer Agenten nach einander“](#), auf Seite 76 oder [„Bereitstellen und Starten mehrerer Agenten gleichzeitig“](#), auf Seite 77.

Bereitstellen und Starten mehrerer Agenten nach einander

Sie können Remote-Installationen durchführen, um mehrere Agenten nach einander bereitzustellen, die eine einzelne Datei `agent.properties` verwenden.

Voraussetzungen

- Prüfen Sie, ob die Voraussetzungen in [„Gleichzeitiges Installieren mehrerer Endpoint Operations Management-Agenten“](#), auf Seite 75 erfüllt werden.

- Prüfen Sie, ob Sie eine standardmäßige Agenteneigenschaftsdatei konfiguriert und diese in die Agenteninstallation oder an einen Speicherort kopiert haben, der für die Agenteninstallation verfügbar ist.

Vorgehensweise

- 1 Melden Sie sich in dem Benutzerkonto auf dem Installationsserver an, das Sie mit Berechtigungen zur Verwendung von SSH für die Herstellung einer Verbindung zu jeder Zielplattform ohne Kennworteingabe konfiguriert haben.
- 2 Verwenden Sie SSH, um eine Verbindung zur Remote-Plattform herzustellen.
- 3 Kopieren Sie das Agentenarchiv zum Agentenhost.
- 4 Entpacken Sie das Agentenarchiv.
- 5 Kopieren Sie die Datei `agent.properties` in das Verzeichnis `AgentHome/conf` des entpackten Agentenarchivs auf der Remote-Plattform.
- 6 Starten Sie den neuen Agenten.

Der Agent registriert sich beim vRealize Operations Manager-Server und führt einen Scan zur automatischen Erkennung durch, um seine Hostplattform und unterstützte verwaltete Produkte zu erkennen, die auf der Plattform laufen.

Bereitstellen und Starten mehrerer Agenten gleichzeitig

Sie können Remote-Installationen durchführen, um Agenten gleichzeitig bereitzustellen, die eine einzelne Datei `agent.properties` verwenden.

Voraussetzungen

- Prüfen Sie, ob die Voraussetzungen in „[Gleichzeitiges Installieren mehrerer Endpoint Operations Management-Agenten](#)“, auf Seite 75 erfüllt werden.
- Prüfen Sie, ob Sie eine standardmäßige Agenteneigenschaftsdatei konfiguriert und diese in die Agenteninstallation oder an einen Speicherort kopiert haben, der für die Agenteninstallation verfügbar ist. Weitere Informationen hierzu finden Sie unter „[Erstellen einer standardmäßigen Endpoint Operations Management-Agenteneigenschaftsdatei](#)“, auf Seite 76.

Vorgehensweise

- 1 Erstellen Sie eine Datei `hosts.txt` auf Ihrem Installationsserver, die den Hostnamen der IP-Adresse jeder Plattform zuordnet, auf der Sie einen Agenten installieren.
- 2 Öffnen Sie eine Befehlszeilenshell auf dem Installationsserver.
- 3 Geben Sie den folgenden Befehl in die Shell ein und geben Sie den korrekten Namen für das Agentenpaket in den Exportbefehl ein.

```
$ export AGENT=epops-agent-x86-64-linux-1.0.0.tar.gz
$ export PATH_TO_AGENT_INSTALL=</path/to/agent/install>
$ for host in `cat hosts.txt`; do scp $AGENT $host:$PATH_TO_AGENT_INSTALL && ssh $host "cd
$PATH_TO_AGENT_INSTALL; tar xzfp $AGENT &&
./epops-agent-1.0.0/ep-agent.sh start"; done
```

- 4 (Optional) Wenn die Zielhosts aufeinanderfolgende Namen haben, z. B. `host001`, `host002`, `host003` usw., können Sie die Datei `hosts.txt` überspringen und den Befehl `seq` verwenden.

```
$ export AGENT=epops-agent-x86-64-linux-1.0.0.tar.gz
$ for i in `seq 1 9`; do scp $AGENT host$i: && ssh host$i "tar xzfp $AGENT &&
./epops-agent-1.0.0/ep-agent.sh start"; done
```

Die Agenten registrieren sich beim vRealize Operations Manager-Server und führen einen Scan zur automatischen Erkennung durch, um ihre Hostplattform und unterstützte verwaltete Produkte zu erkennen, die auf der Plattform laufen.

Rollen und Berechtigungen in vRealize Operations Manager

vRealize Operations Manager bietet mehrere vordefinierte Rollen für die Zuweisung von Berechtigungen zu Benutzern. Sie können auch eigene Rollen erstellen.

Sie müssen über Berechtigungen verfügen, um Zugriff auf bestimmte Funktionen in der vRealize Operations Manager-Benutzeroberfläche zu haben. Die Ihrem Benutzerkonto zugeordneten Rollen legen fest, auf welche Funktionen Sie zugreifen und welche Aktionen Sie ausführen können.

Jede vordefinierte Rolle umfasst einen Satz von Berechtigungen für Benutzer zur Durchführung von Erstellungs-, Lese-, Aktualisierungs- und Löschaktionen auf Komponenten wie z. B. Dashboards, Berichte, Verwaltung, Kapazität, Richtlinien, Probleme, Symptome, Warnungen, Benutzerkontenverwaltung und Adapter.

Administrator	Beinhaltet Berechtigungen für alle Funktionen, Objekte und Aktionen in vRealize Operations Manager.
PowerUser	Benutzer dürfen Aktionen der Administratorrolle durchführen, haben aber keine Berechtigungen zur Benutzer- und Clusterverwaltung. vRealize Operations Manager ordnet vCenter Server-Benutzer dieser Rolle zu.
PowerUserMinusRemediation	Benutzer dürfen Aktionen der Administratorrolle durchführen, haben aber keine Berechtigungen zur Benutzer- und Clusterverwaltung und für Standardisierungsaktionen.
ContentAdmin	Benutzer dürfen alle Inhalte einschließlich Ansichten, Berichte, Dashboards und benutzerdefinierte Gruppen in vRealize Operations Manager verwalten.
AgentManager	Benutzer können Endpoint Operations Management bereitstellen und konfigurieren.
GeneralUser-1 bis GeneralUser-4	Diese vordefinierten Vorlagenrollen sind anfangs als ReadOnly-Rollen definiert. vCenter Server-Administratoren können diese Rollen zur Erstellung von Rollenkombinationen konfigurieren, um Benutzern verschiedene Berechtigungsarten zu gewähren. Rollen werden während der Registrierung einmalig mit vCenter Server synchronisiert.
ReadOnly	Benutzer verfügen lediglich über schreibgeschützten Zugriff und können Lesevorgänge, jedoch keine Schreibvorgänge zum Erstellen, Aktualisieren oder Löschen durchführen.

Registrieren von Agenten auf Clustern

Sie können die Registrierung von Agenten auf Clustern optimieren, indem Sie einen DNS-Namen für ein Cluster definieren und dieses Cluster so konfigurieren, dass die Metriken nach einander in einer Schleife geteilt werden.

Sie müssen den Agenten nur auf dem DNS registrieren, nicht in der IP-Adresse jeder einzelnen Maschine im Cluster. Wenn Sie den Agenten in jedem Knoten im Cluster registrieren, wirkt sich das auf den Umfang Ihrer Umgebung aus.

Wenn Sie das Cluster so konfiguriert haben, dass die empfangenen Metriken in einer aufeinander folgenden Schleife geteilt werden, und wenn der Agent vom DNS-Server eine IP-Adresse abfragt, dann entspricht die angegebene IP-Adresse einer der virtuellen Maschinen im Cluster. Wenn der Agent den DNS das nächste Mal abfragt, wird die IP-Adresse der nächsten virtuellen Maschine im Cluster angegeben, und so weiter. Die geclusterten Maschinen sind in einer Schleifenkonfiguration angeordnet, sodass jede Maschine abwechselnd Metriken empfängt und für eine ausgeglichene Last gesorgt wird.

Nachdem Sie den DNS konfiguriert haben, ist es wichtig, ihn zu warten, damit sichergestellt wird, dass die IP-Adressen hinzugefügter oder entfernter Maschinen entsprechend aktualisiert werden.

Manuelles Erstellen von Betriebssystemobjekten

Der Agent erkennt einige der Objekte, die er überwachen soll, automatisch. Sie können andere Objekte wie Dateien, Skripte oder Prozesse manuell hinzufügen und die Details festlegen, damit der Agent diese überwachen kann.

Die Aktion **Betriebssystemobjekt überwachen** erscheint nur im Menü **Aktionen** eines Objekts, das ein übergeordnetes Objekt sein kann.

Vorgehensweise

- 1 Wählen Sie im linken Bereich des vRealize Operations Manager das Agentenadapterobjekt aus, das das übergeordnete Objekt sein soll, unter dem Sie ein BS-Objekt erstellen.
- 2 Wählen Sie **Aktionen > BS-Objekt überwachen** aus.
Eine Liste der kontextsensitiven übergeordneten Objekte wird im Menü angezeigt.
- 3 Wählen Sie eine der folgenden Optionen aus:
 - Klicken Sie auf einen Objekttyp in der Liste, um das Dialogfeld „BS-Objekt überwachen“ für diesen Objekttyp zu öffnen.
In der Liste werden die drei am häufigsten ausgewählten Objekttypen angezeigt.
 - Wenn der gewünschte Objekttyp in der Liste nicht angezeigt wird, klicken Sie auf **Mehr**, um das Dialogfeld „BS-Objekt überwachen“ zu öffnen, und wählen Sie im Menü **Objekttyp** den Objekttyp aus der vollständigen Liste der wählbaren Objekte aus.
- 4 Legen Sie einen Anzeigenamen für das BS-Objekt fest.
- 5 Geben Sie die entsprechenden Werte in die anderen Textfelder ein.
Die Optionen im Menü werden entsprechend dem ausgewählten Objekttyp gefiltert.
Einige Textfelder können Standardwerte anzeigen, die Sie bei Bedarf überschreiben können. Beachten Sie die folgenden Informationen über Standardwerte.

Option	Wert
Vorgang	<p>Bereitstellung einer PTQL-Abfrage im Format: <code>Class.Attribute.operator=value</code>. Beispielsweise <code>Pid.PidFile.eq=/var/run/sshd.pid</code>. Wobei:</p> <ul style="list-style-type: none"> ■ <code>Class</code> der Name der Sigar-Klasse ohne Proc-Präfix ist. ■ <code>Attribute</code> ein Attribut einer bestimmten Klasse, Index eines Arrays oder Schlüssel in einer Map-Klasse ist. ■ <code>operator</code> eins der Folgenden ist (für Zeichenfolgenwerte): <ul style="list-style-type: none"> ■ <code>eq</code> gleich dem Wert ■ <code>ne</code> ungleich dem Wert ■ <code>ew</code> endet mit dem Wert ■ <code>sw</code> beginnt mit dem Wert ■ <code>ct</code> enthält den Wert (Substring) ■ <code>re</code> Wert stimmt mit regulärem Ausdruck überein <p>Das Komma wird als Trennzeichen für Abfragen verwendet.</p>
Windows-Dienst	<p>Überwacht eine Anwendung, die als Dienst unter Windows ausgeführt wird. Zur Konfiguration geben Sie den Dienstnamen in Windows an. So ermitteln Sie den Dienstnamen:</p> <ol style="list-style-type: none"> 1 Wählen Sie im Windows-Startmenü Ausführen. 2 Geben Sie in das Dialogfeld <code>services.msc</code> ein und klicken Sie auf OK. 3 Klicken Sie mit der rechten Maustaste in der Liste der angezeigten Dienste auf den zu überwachen- den Dienst und wählen Sie Eigenschaften. 4 Sie finden den Dienstnamen auf der Registerkarte Allgemein.
Skript	Konfigurieren Sie vRealize Operations Manager, um regelmäßig ein Skript auszuführen, das eine Sys- tem- oder Anwendungsmetrik erfasst.

6 Klicken Sie auf **OK**.

Sie können erst auf **OK** klicken, wenn Sie Werte in alle erforderlichen Textfelder eingegeben haben.

Das BS-Objekt wird unter seinen übergeordneten Objekt angezeigt und die Überwachung beginnt.



VORSICHT Wenn Sie bei der Erstellung eines BS-Objekts ungültige Details eingeben, wird das Objekt er- stellt, aber der Agent kann es nicht erkennen und die Metriken werden nicht gesammelt.

Verwalten von Objekten mit fehlenden Konfigurationsparametern

Manchmal, wenn ein Objekt zum ersten Mal von vRealize Operations Manager erkannt wird, wird die Feh- len von Werten für einige obligatorische Konfigurationsparameter erkannt. Sie können die Objektparameter bearbeiten, um die fehlenden Werte bereitzustellen.

Wenn Sie in vRealize Operations Manager in der Ansicht „Umgebungsüberblick“ **Benutzerdefinierte Grup- pen > Objekte mit fehlender Konfiguration (EP Ops)** auswählen, wird eine Liste aller Objekte mit fehlen- den obligatorischen Konfigurationsparametern angezeigt. Außerdem geben Objekte mit fehlenden Parame- tern einen Fehler in den Erfassungsstatusdaten zurück.

Wenn Sie ein Objekt mit fehlenden Konfigurationsparametern auf der Benutzeroberfläche von vRealize Operations Manager auswählen, wird auf der Menüleiste ein rotes Symbol für den fehlenden Kon- figurationsstatus angezeigt. Wenn Sie mit der Maus auf das Symbol zeigen, werden Einzelheiten zu diesem Problem angezeigt.

Sie können die fehlenden Parameterwerte über den Menübefehl **Aktion > Objekt bearbeiten** ergänzen.

Zuordnen virtueller Maschinen zu Betriebssystemen

Sie können Ihre virtuellen Maschinen einem Betriebssystem zuordnen, um zusätzliche Informationen anzugeben, die Sie bei der Bestimmung der Hauptursache für die Auslösung einer Warnung für eine virtuelle Maschine unterstützen.

vRealize Operations Manager überwacht Ihre ESXi-Hosts und die darauf befindlichen virtuellen Maschinen. Wenn Sie einen Endpoint Operations Management-Agenten bereitstellen, erkennt er die virtuelle Maschine und die Objekte, die darauf laufen. Durch die Korrelation der vom Endpoint Operations Management-Agenten erkannten virtuellen Maschinen mit den Betriebssystemen, die von vRealize Operations Manager überwacht werden, erhalten Sie mehr Details, um die exakte Ursache einer ausgelösten Warnung zu bestimmen.

Vergewissern Sie sich, dass Sie den vCenter Adapter mit dem vCenter Server konfiguriert haben, der die virtuellen Maschinen verwaltet. Sie müssen ebenfalls sicherstellen, dass VMware Tools mit dem vCenter Server kompatibel ist, der auf jeder der virtuellen Maschinen installiert ist.

Benutzerszenario

vRealize Operations Manager wird ausgeführt, aber Sie haben den Endpoint Operations Management-Agenten in Ihrer Umgebung noch nicht bereitgestellt. Sie haben vRealize Operations Manager so konfiguriert, dass im Fall von CPU-Problemen Warnungen gesendet werden. Sie sehen eine Warnung auf Ihrem Dashboard, weil in einer der virtuellen Maschinen, die auf einem Linux-Betriebssystem läuft, nicht ausreichend CPU-Kapazität zur Verfügung steht. Sie stellen zwei weitere virtuelle CPUs bereit, aber die Warnung bleibt bestehen. Sie können nicht herausfinden, wodurch das Problem hervorgerufen wird.

Wenn Sie in dieser Situation den Endpoint Operations Management-Agenten bereitgestellt hätten, können Sie die Objekte auf Ihren virtuellen Maschinen sehen und feststellen, dass ein Anwendungstypobjekt die gesamte verfügbare CPU-Kapazität verbraucht. Wenn Sie mehr CPU-Kapazität hinzufügen, wird auch diese verbraucht. Sie deaktivieren das Objekt und die CPU-Verfügbarkeit stellt kein Problem mehr dar.

Anzeigen von Objekten auf virtuellen Maschinen

Nachdem Sie einen Endpoint Operations Management-Agenten auf einer virtuellen Maschine bereitgestellt haben, wird die Maschine dem Betriebssystem zugeordnet und Sie können alle Objekte auf dieser Maschine sehen.

Alle Aktionen und Ansichten, die für andere Objekte in Ihrer vRealize Operations Manager-Umgebung verfügbar sind, stehen auch für die neu erkannten Server-, Service- und Anwendungsobjekte sowie für den bereitgestellten Agenten zur Verfügung.

Sie sehen die Objekte auf einer virtuellen Maschine in der Bestandsliste, wenn Sie die Maschine in der Ansicht **Umgebung > vSphere-Hosts und -Cluster** auswählen. Sie sehen die Objekte und den bereitgestellten Agenten unter dem Betriebssystem.

Wenn Sie ein Objekt auswählen, werden im mittleren Bereich der Benutzeroberfläche Daten für diese Objekte angezeigt.

Installieren optionaler Lösungen in vRealize Operations Manager

Sie können die Überwachungsfunktionen von vRealize Operations Manager erweitern, indem Sie optionale Lösungen von VMware oder Drittanbietern installieren.

VMware-Lösungen umfassen Adapter für Speichergeräte, Log Insight, NSX für vSphere, Netzwerkgeräte und VCM. Zu den Lösungen von Drittanbietern zählen AWS, SCOM, EMC Smarts und viele andere. Um Software und Dokumentation für optionale Lösungen herunterzuladen, besuchen Sie [VMware Solution Exchange](#).

Lösungen können Dashboards, Berichte, Warnungen und andere Inhalte sowie Adapter enthalten. Mit Adaptern verwaltet vRealize Operations Manager die Kommunikation und Integration mit anderen Produkten, Anwendungen und Funktionen. Wenn ein Management Pack installiert ist und die Lösungsadapter konfiguriert sind, können Sie die Analyse- und Warnungstools von vRealize Operations Manager verwenden, um die Objekte in Ihrer Umgebung zu verwalten.

Wenn Sie ein Upgrade von einer früheren Version von vRealize Operations Manager durchführen, werden die Management Pack-Dateien in die Datei `/usr/lib/vmware-vcops/user/plugins/.backup` kopiert, die sich in einem Ordner befindet, dessen Name aus dem Datum und der Uhrzeit besteht. Bevor Sie Ihre Daten zu der neuen vRealize Operations Manager-Instanz migrieren, müssen Sie die neuen Adapter im Arbeitsbereich **Verwaltung > Lösungen** konfigurieren. Falls der Adapter angepasst wurde, werden die Adapteranpassungen bei der Migration nicht berücksichtigt und müssen neu konfiguriert werden.

Wenn Sie ein Management Pack in vRealize Operations Manager auf eine neuere Version aktualisieren und den Adapter angepasst haben, sind die Adapteranpassungen im Upgrade nicht enthalten und müssen neu konfiguriert werden.

Verwalten der Anmeldedaten für Lösungen

Anmeldeinformationen sind die Benutzerkonten, die vRealize Operations Manager verwendet, um eine oder mehrere Lösungen und die zugehörigen Adapter zu aktivieren und die Kommunikation mit den Ziel-datenquellen einzurichten. Die Anmeldeinformationen werden beim Konfigurieren der einzelnen Adapter bereitgestellt. Verwenden Sie die Option „Anmeldedaten“, wenn Sie die Einstellungen außerhalb des Adapterkonfigurationsvorgangs hinzufügen oder ändern und Änderungen an Ihrer Umgebung vornehmen möchten.

Wenn Sie vorhandene Anmeldeinformationen ändern, beispielsweise, um Änderungen basierend auf Ihrer Kennwortrichtlinie zu übernehmen, verwenden die mit diesen Anmeldeinformationen konfigurierten Adapter den neuen Benutzernamen und das Kennwort für die Kommunikation zwischen vRealize Operations Manager und dem Zielsystem.

Die Verwaltung der Anmeldeinformationen wird häufig zudem dazu verwendet, fehlerhaft konfigurierte Anmeldeinformationen zu entfernen. Wenn Sie gültige Anmeldeinformationen löschen, die aktiv von einem Adapter verwendet werden, deaktivieren Sie die Kommunikation zwischen den zwei Systemen.

Falls eine Änderung der konfigurierten Anmeldedaten erforderlich ist, um Veränderungen in Ihrer Umgebung zu berücksichtigen, können Sie Einstellungen wie z. B. den Namen, den Benutzernamen und das Kennwort bzw. den Zugangscode und den Kennwortsatz bearbeiten, ohne eine neue Adapterinstanz für das Zielsystem konfigurieren zu müssen. Sie können Einstellungen der Anmeldedaten durch Klicken auf **Verwaltung** und dann auf **Anmeldedaten** bearbeiten.

Alle Adapter-Anmeldedaten, die Sie hinzufügen, werden mit anderen Adapter-Administratoren und vRealize Operations Manager-Collector-Hosts gemeinsam genutzt. Andere Administratoren können diese Anmeldedaten verwenden, um eine neue Adapterinstanz zu konfigurieren oder eine Adapterinstanz auf einen neuen Host zu verschieben.

Anmeldedaten verwalten

Für die Konfiguration oder Neukonfiguration von Anmeldedaten, mit denen Sie eine Adapterinstanz aktivieren, müssen Sie die Erfassungskonfigurations-Einstellungen wie z. B. einen Benutzernamen und ein Kennwort angeben, die im Zielsystem gültig sind. Darüber hinaus können Sie die Verbindungseinstellungen für eine vorhandene Anmeldedateninstanz ändern.

Zugriff auf das Dialogfeld „Anmeldedaten verwalten“

Klicken Sie im linken Bereich auf das Symbol **Verwaltung** und klicken Sie dann auf **Anmeldedaten**. Klicken Sie auf das Pluszeichen, um neue Anmeldedaten hinzuzufügen, oder auf den Stift, um die ausgewählten Anmeldedaten zu bearbeiten.

Optionen im Dialogfeld „Anmeldedaten verwalten“

Im Dialogfeld „Anmeldedaten verwalten“ werden neue Adapteranmeldedaten hinzugefügt oder vorhandene Adapteranmeldedaten geändert. Dieses Dialogfeld variiert in Abhängigkeit vom Adaptertyp und davon, ob Sie Adapteranmeldedaten hinzufügen oder bearbeiten. Nachfolgend werden die grundlegenden Optionen beschrieben. Welche anderen als die grundlegenden Optionen verfügbar sind, hängt von der Lösung ab.



VORSICHT Alle Adapter-Anmeldedaten, die Sie hinzufügen, werden mit anderen Adapter-Administratoren und vRealize Operations Manager-Collector-Hosts gemeinsam genutzt. Andere Administratoren können diese Anmeldedaten verwenden, um eine neue Adapterinstanz zu konfigurieren oder eine Adapterinstanz auf einen neuen Host zu verschieben.

Tabelle 7-4. Optionen zum Hinzufügen oder Bearbeiten im Dialogfeld „Anmeldedaten verwalten“

Option	Beschreibung
Adaptertyp	Der Adaptertyp, für den Sie die Anmeldedaten konfigurieren.
Anmeldedatenart	Die dem Adapter zugeordneten Anmeldedaten. Die Kombination aus Adapter und Anmeldedatentyp wirkt sich auf die zusätzlichen Konfigurationsoptionen aus.
Anmeldedatenname	Der beschreibende Name, unter dem Sie die Anmeldedaten verwalten.
Benutzername	Kontoanmeldedaten, die in der Adapterkonfiguration zum Herstellen einer Verbindung von vRealize Operations Manager mit dem Zielsystem verwendet werden.
Kennwort	Kennwort für die angegebenen Anmeldedaten.

Verwalten von Collector-Gruppen

vRealize Operations Manager verwendet Collectors zur Verwaltung von Adapter-Prozessen, wie z. B. die Erfassung von Metriken von Objekten. Beim Konfigurieren einer Adapterinstanz können Sie einen Collector oder eine Collector-Gruppe auswählen.

Wenn sich Remote-Collectors in Ihrer Umgebung befinden, können Sie eine neue Collector-Gruppe erstellen und Remote-Collectors der Gruppe hinzufügen. Wenn Sie einen Adapter einer Collector-Gruppe zuweisen, kann der Adapter beliebige Collectors in der Gruppe verwenden. Mithilfe von Collector-Gruppen können Sie Adapter-Ausfallsicherheit in den Fällen erreichen, in denen der Collector von Netzwerkunterbrechungen betroffen oder nicht mehr verfügbar ist. Wenn in einem solchen Fall der Collector Teil einer Gruppe ist, wird die gesamte Arbeitslast auf die Collectors in der Gruppe verteilt, d. h., die Arbeitslast des einzelnen Collectors wird reduziert.

Migrieren einer vCenter Operations Manager-Bereitstellung in diese Version

Durch den Import von Daten kann eine eingerichtete oder eine Produktionsversion von vRealize Operations Manager die Überwachung einer vCenter Operations Manager-Bereitstellung übernehmen.

Sie können vCenter Operations Manager nicht direkt zu dieser Version von vRealize Operations Manager migrieren. Befolgen Sie stattdessen diese zwei Prozessschritte:

- 1 Migrieren und importieren Sie vCenter Operations Manager 5.8x zu vRealize Operations Manager 6.0.x, wie in der Dokumentation für Version 6.0.x beschrieben.

- 2 Verwenden Sie die vRealize Operations Manager-Option **Software-Update**, um ein Update von vRealize Operations Manager 6.0.x zu dieser Version durchzuführen.

HINWEIS Vergewissern Sie sich, dass sich Ihre vCenter Operations Manager 5.8.x- und vRealize Operations Manager 6.0.x-Instanzen auf demselben physischen Netzwerk befinden. Andernfalls funktioniert der Datenimport unter Umständen nicht.

Überlegungen nach der Installation von vRealize Operations Manager

8

Nachdem Sie die Installation von vRealize Operations Manager vorgenommen haben, sind gegebenenfalls Nacharbeiten durchzuführen, denen Sie Ihre Aufmerksamkeit widmen sollten.

Dieses Kapitel behandelt die folgenden Themen:

- „Grundlegendes zum Anmelden bei vRealize Operations Manager“, auf Seite 85
- „Das Programm zur Verbesserung der Kundenerfahrung“, auf Seite 86

Grundlegendes zum Anmelden bei vRealize Operations Manager

Zum Anmelden bei vRealize Operations Manager müssen Sie einen Webbrowser auf den vollqualifizierten Domännennamen (FQDN) oder die IP-Adresse eines Knotens im vRealize Operations Manager-Cluster verweisen.

Wenn Sie sich bei vRealize Operations Manager anmelden, sollten Sie einige Dinge berücksichtigen.

- Nach der Erstkonfiguration lautet die URL der Produktschnittstelle:
`https://Knoten-FQDN-oder-IP-Adresse`
- Vor der Erstkonfiguration wird über die Produkt-URL stattdessen die Verwaltungsschnittstelle geöffnet.
- Nach der Erstkonfiguration lautet die URL der Verwaltungsschnittstelle:
`https://Knoten-FQDN-oder-IP-Adresse/admin`
- Der Name des Administratorkontos lautet „admin“. Der Kontoname kann nicht geändert werden.
- Das Administratorkonto unterscheidet sich vom Root-Konto, das für die Anmeldung an der Konsole verwendet wird, und es hat nicht dasselbe Passwort.
- Während Sie bei der Verwaltungsschnittstelle angemeldet sind, vermeiden Sie es, den Knoten, bei dem Sie angemeldet sind, offline zu schalten und herunterzufahren. Andernfalls wird die Schnittstelle geschlossen.
- Die Anzahl der gleichzeitigen Anmeldungen, nach der eine Leistungsabnahme bemerkbar ist, ist abhängig von Faktoren wie der Anzahl der Knoten im Analyse-Cluster, der Größe dieser Knoten und der Last, die jede Benutzersitzung voraussichtlich auf dem System erzeugen wird. Starke Nutzer führen unter Umständen viele administrative Aktivitäten, mehrere gleichzeitige Dashboards, Cluster-Managementaufgaben usw. aus. Geringe Nutzer sind häufiger und benötigen häufig nur ein oder zwei Dashboards.

Das Größearbeitsblatt für Ihre Version von vRealize Operations Manager enthält weitere Angaben zur Unterstützung gleichzeitiger Anmeldungen. Weitere Informationen hierzu finden Sie im [Knowledgebase-Artikel 2093783](#).

- Sie können sich mit vRealize Operations Manager-internen Benutzerkonten, wie etwa dem Maintenance-Admin-Konto, nicht bei einer vRealize Operations Manager-Schnittstelle anmelden.
- Sie können die Produktoberfläche nicht von einem Remote-Controller-Knoten aus öffnen, aber Sie Verwaltungsschnittstelle öffnen.
- Informationen zu unterstützten Webbrowsern finden Sie in den Versionshinweisen für Ihre vRealize Operations Manager-Version.

Das Programm zur Verbesserung der Kundenerfahrung

Dieses Produkt nimmt am Programm zur Verbesserung der Kundenerfahrung (CEIP) von VMware teil. CEIP liefert VMware Informationen, mit denen VMware seine Produkte und Dienstleistungen verbessern, Probleme beheben und Sie bezüglich der optimalen Bereitstellung und Verwendung unserer Produkte beraten kann. Sie können jederzeit an CEIP für vRealize Operations Manager teilnehmen und das Programm jederzeit verlassen.

Details zur Datenerfassung über CEIP und den Zweck ihrer Verwendung durch VMware finden Sie im Trust & Assurance Center unter <http://www.vmware.com/trustvmware/ceip.html>.

Teilnahme am Programm zur Verbesserung der Kundenerfahrung für vRealize Operations Manager oder Verlassen des Programms

Sie können jederzeit am Programm zur Verbesserung der Kundenerfahrung (CEIP) für vRealize Operations Manager teilnehmen und das Programm jederzeit verlassen.

vRealize Operations Manager bietet Ihnen die Möglichkeit, am Programm zur Verbesserung der Kundenerfahrung (CEIP) teilzunehmen, wenn Sie das Produkt erstmalig installieren oder konfigurieren. Nach der Installation können Sie am Programm teilnehmen oder es verlassen, indem Sie diese Schritte befolgen.

Vorgehensweise

- 1 Klicken Sie im vRealize Operations Manager auf **Verwaltung**.
- 2 Wählen Sie **Globale Einstellungen**.
- 3 Klicken Sie in der Symbolleiste auf das Symbol **Bearbeiten**.
- 4 Aktivieren oder deaktivieren Sie die Option **Programm zur Verbesserung der Kundenzufriedenheit**.
Wenn diese Option aktiviert ist, wird das Programm aktiviert und es werden Daten an <https://vmware.com> gesendet.
- 5 Klicken Sie auf **OK**.

Aktualisieren Ihrer Software

Sie können Ihre vorhandenen vRealize Operations Manager-Bereitstellungen auf eine neu veröffentlichte Version aktualisieren.

Wenn Sie eine Softwareaktualisierung durchführen, müssen Sie sicherstellen, dass Sie die korrekte PAK-Datei für Ihr Cluster verwenden. Es empfiehlt sich, einen Snapshot des Clusters zu erstellen, bevor Sie die Software aktualisieren. Denken Sie jedoch daran, den Snapshot nach Abschluss der Aktualisierung zu löschen.

Falls Sie die von vRealize Operations Manager bereitgestellten Inhalte wie Warnungen, Symptome, Empfehlungen und Richtlinien angepasst haben und nun Updates für diese Inhalte installieren möchten, klonen Sie diese Inhalte vor der Durchführung der Aktualisierung. Auf diese Weise erhalten Sie die Möglichkeit, bei der Update-Installation Standardinhalte wiederherzustellen. Das Update kann dann neue Inhalte bereitstellen, ohne die benutzerdefinierten Inhalte zu überschreiben.

Dieses Kapitel behandelt die folgenden Themen:

- [„Ermitteln der PAK-Datei für das Software-Update“](#), auf Seite 87
- [„Erstellen eines Snapshots im Rahmen eines Updates“](#), auf Seite 88
- [„Installieren eines Software-Updates“](#), auf Seite 89

Ermitteln der PAK-Datei für das Software-Update

Jeder Typ der Clusteraktualisierung erfordert eine spezifische PAK-Datei. Vergewissern Sie sich, dass Sie die korrekte Datei verwenden.

Korrekte PAK-Dateien herunterladen

Um Ihre vRealize Operations Manager-Umgebung zu aktualisieren, müssen Sie die richtige PAK-Datei für die Cluster herunterladen, die aktualisiert werden sollen. Beachten Sie, dass nur die Virtual Appliance-Cluster eine PAK-Datei für die Aktualisierung des Betriebssystems verwenden. Hostnameneinträge im Verzeichnis `/etc/hosts` jedes Knotens werden möglicherweise zurückgesetzt, wenn die PAK-Datei zur Aktualisierung des Betriebssystems für ein Update von vRealize Operations 6.0.x auf Version 6.1 angewendet wird. Sie können die Hostdatei nach Abschluss des Software-Updates manuell aktualisieren.

Tabelle 9-1. Spezifische PAK-Dateien für unterschiedliche Clustertypen

Clustertyp	Aktualisierung des Betriebssystems	Produktaktualisierung
Virtual Appliance-Cluster. Verwenden Sie die PAK-Dateien für die Aktualisierung des Betriebssystems und des Produkts.	vRealize_Operations_Manager-VA-OS-xxx.pak	vRealize_Operations_Manager-VA-xxx.pak
Heterogene Virtual Appliance-Cluster. Verwenden Sie die PAK-Dateien für die Aktualisierung des Betriebssystems und des Produkts.	vRealize_Operations_Manager-VA-OS-xxx.pak	vRealize_Operations_Manager-VA-WIN-xxx.pak
Eigenständige RHEL-Cluster.		vRealize_Operations_Manager-RHEL-xxx.pak
Heterogene RHEL-Cluster. Verwenden Sie diese Datei, wenn Sie ein heterogenes Cluster mit RHEL-Knoten und Windows Remote-Collectors haben.		vRealize_Operations_Manager-RHEL-WIN-xxx.pak
Windows Cluster		vRealize_Operations_Manager-WIN-xxx.pak

Erstellen eines Snapshots im Rahmen eines Updates

Es wird empfohlen, einen Snapshot für jeden Knoten im Cluster zu erstellen, bevor Sie ein vRealize Operations Manager-Cluster aktualisieren. Nachdem das Update abgeschlossen ist, müssen Sie den Snapshot löschen, um eine Beeinträchtigung der Leistung zu vermeiden.

Informationen über Snapshots finden Sie in der Dokumentation zur Verwaltung virtueller Maschinen in vSphere.

Vorgehensweise

- 1 Melden Sie sich an der vRealize Operations Manager-Verwaltungsschnittstelle als `https://<master-node-FQDN-or-IP-address>/admin` an.
- 2 Wählen Sie einen Knoten im Cluster aus.
- 3 Klicken Sie auf **Offline stellen**.
Wiederholen Sie diesen Vorgang für jeden Knoten.
- 4 Wenn alle Knoten offline sind, öffnen Sie den vSphere-Client.
- 5 Klicken Sie mit der rechten Maustaste auf eine virtuelle vRealize Operations Manager-Maschine.
- 6 Klicken Sie auf **Snapshot** und anschließend auf **Snapshot erstellen**.
 - a Benennen Sie den Snapshot. Verwenden Sie einen aussagekräftigen Namen wie „Vor-Update.“
 - b Deaktivieren Sie das Kontrollkästchen **Snapshot des Arbeitsspeichers der virtuellen Maschine**.
 - c Deaktivieren Sie das Kontrollkästchen **Quiesce-Gastdateisystem gewährleisten (VMware Tools muss installiert sein)**.
 - d Klicken Sie auf **OK**.
- 7 Wiederholen Sie diese Schritte für jeden Knoten im Cluster.

Weiter

Starten Sie die Aktualisierungsvorgang wie in „[Installieren eines Software-Updates](#)“, auf Seite 89 beschrieben.

Installieren eines Software-Updates

Wenn Sie vRealize Operations Manager bereits installiert haben, können Sie Ihre Software aktualisieren, wenn eine neuere Version zur Verfügung steht.

HINWEIS Die Installation kann mehrere Minuten oder sogar Stunden dauern, je nach Größe und Typ Ihrer Cluster und Knoten.

Voraussetzungen

- Erstellen Sie einen Snapshot jedes Knotens im Cluster. Informationen zum Durchführen dieser Aufgaben finden Sie im vRealize Operations Manager-Informationscenter.
- Ermitteln Sie die PAK-Datei für Ihr Cluster. Informationen darüber, welche Datei verwendet werden muss, finden Sie im vRealize Operations Manager-Informationscenter.
- Bevor Sie die PAK-Datei installieren oder ein Upgrade der vRealize Operations Manager-Instanz durchführen, klonen Sie alle angepassten Inhalte, um sie beizubehalten. Zu den angepassten Inhalten können Warnungsdefinitionen, Symptomdefinitionen, Empfehlungen und Ansichten zählen. Anschließend wählen Sie während des Software-Updates die Optionen **Installieren Sie die PAK-Datei, selbst wenn sie bereits installiert ist** und **Auf Standard zurücksetzen** aus.
- Für den Aktualisierungsvorgang der Version 6.2.1 von vRealize Operations Manager gibt es einen Validierungsprozess, in dem Probleme ermittelt werden, bevor Sie mit der Aktualisierung der Software beginnen. Obwohl es sinnvoll ist, die Prüfung vor der Aktualisierung durchzuführen und gefundene Probleme zu beheben, können Benutzer mit umgebungsbedingten Einschränkungen diese Validierungsprüfung deaktivieren.

Führen Sie die folgenden Schritte aus, um die Validierungsprüfung vor der Aktualisierung zu deaktivieren:

- Bearbeiten Sie die folgende Aktualisierungsdatei: `/storage/db/pakRepoLocal/bypass_pre-checks_vRealizeOperationsManagerEnterprise-buildnumberofupdate.json`.
- Ändern Sie den Wert in TRUE und führen Sie die Aktualisierung aus.

HINWEIS Wenn Sie die Validierung deaktivieren, treten möglicherweise während des Aktualisierungsvorgangs blockierende Fehler auf.

Vorgehensweise

- 1 Melden Sie sich an der vRealize Operations Manager-Verwaltungsschnittstelle des Masterknotens Ihres Clusters unter `https://master-node-FQDN-or-IP-address/admin` an.
- 2 Klicken Sie im linken Bereich auf **Software-Update**.
- 3 Klicken Sie im Hauptbereich auf **Software-Update installieren**.

- 4 Befolgen Sie die Schritte im Assistenten, um Ihre PAK-Datei zu lokalisieren und zu installieren.
 - a Wenn Sie eine Virtual Appliance-Bereitstellung aktualisieren, führen Sie die Aktualisierung des Betriebssystems aus.
Dadurch wird das Betriebssystem auf der virtuellen Appliance aktualisiert und jede virtuelle Maschine neu gestartet.
 - b Installieren Sie die PAK-Datei für die Produktaktualisierung.
Warten Sie, bis die Softwareaktualisierung abgeschlossen ist. Wenn dies der Fall ist, werden Sie von der Verwaltungsschnittstelle abgemeldet.
- 5 Melden Sie sich wieder bei der Verwaltungsschnittstelle des Masterknotens an.
Die Hauptseite „Clusterstatus“ wird angezeigt und das Cluster wird automatisch online gestellt. Auf der Statusseite wird ebenfalls die Schaltfläche „Online stellen“ angezeigt. Auf diese Schaltfläche sollten Sie jedoch nicht klicken.
- 6 Löschen Sie den Cache des Browsers, und falls die Browserseite nicht automatisch neu geladen wird, aktualisieren Sie die Anzeige der Seite.
Der Clusterstatus ändert sich in "Wechsel in den Online-Zustand". Wenn der Clusterstatus sich in "Online" ändert, ist das Upgrade abgeschlossen.

HINWEIS Wenn ein Cluster ausfällt und sich der Status während der Installation einer PAK-Dateiaktualisierung in „Offline“ ändert, stehen einige Knoten nicht mehr zur Verfügung. Um dieses Problem zu beheben, öffnen Sie die Verwaltungsschnittstelle und nehmen Sie das Cluster manuell „Offline“. Klicken Sie anschließend auf **Installation beenden**, um die Installation fortzusetzen.

- 7 Klicken Sie auf **Software-Update**, um zu überprüfen, ob die Aktualisierung durchgeführt wurde.
Im Hauptbereich wird eine Meldung angezeigt, dass die Aktualisierung erfolgreich abgeschlossen wurde.

Weiter

Löschen Sie die Snapshots, die Sie vor der Softwareaktualisierung erstellt haben.

HINWEIS Mehrere Snapshots können die Leistung beeinträchtigen, weshalb Sie die vor der Aktualisierung erstellten Snapshots nach Abschluss der Softwareaktualisierung löschen sollten.

Index

A

- Adapter
 - Anmeldedaten **82**
 - Collector-Gruppe **83**
 - vCenter Server **37**
- Agent
 - Clientzertifikat **70**
 - Installation und Bereitstellung **39**
 - Registrieren **70**
 - Starten Sie den Launcher von einer Linux Befehlszeile aus **71**
 - Starten Sie den Launcher von einer Windows Befehlszeile aus **71**
- Agent installieren, Java-Voraussetzungen **47**
- Agenten
 - auf Linux-Plattform installieren **41, 43**
 - auf Windows-Plattform installieren **44**
 - Clientzertifikat **69**
 - Datei agent.properties **54**
 - Deinstallieren **73, 74**
 - Eigenschaften **54**
 - Installation ohne Benutzereingaben **54**
 - mehrere Agenten gleichzeitig installieren **75**
 - Neuinstallieren **73, 75**
 - Registrieren **69**
 - Registrieren eines Clusters **78**
 - Starten über eine Befehlszeile **71**
 - Überschreiben von Eigenschaften **53**
 - unbeaufsichtigt auf Windows-Plattform installieren **46**
- Agenteneigenschaften
 - agent.keystore.alias **57**
 - agent.listenPort **58**
 - agent.setup.camSecure-Eigenschaft **62**
 - agent.setup.resetupToken **62**
 - für agenteninitiierte Kommunikation konfigurieren **50**
 - für mehrere Agenten **75, 76**
 - für serverinitiierte Kommunikation konfigurieren **50**
 - Installation ohne Benutzereingaben **50**
 - Kommunikationseigenschaften aktivieren **50**
 - konfigurieren **49**
 - sigar.mirror.procnets **69**
 - sigar.pdh.enableTranslation **69**
- Aktionen, Benutzerzugriff **38**

- Aktualisieren **83, 87**
- AktualisierenAktualisieren **87**
- Anfängliche Einrichtung **33**
- Anforderungen
 - Clusterknoten **10, 12**
 - Zertifikate **16**
- angepasste Zertifikate **16**
- Anmeldedaten, Adapter **82**
- Anmelden **85**

B

- Beispiele, Zertifikatsinhalt **17**
- Benutzerzugriff
 - Aktionen **38**
 - vCenter Server-Aktionen **38**
- Berechtigungen **78**
- Best Practices, Clusterknoten **13**

C

- Cluster
 - Allgemeine Anforderungen **10**
 - Best Practices **13**
 - Netzwerkanforderungen **12**
 - Registrieren eines Agenten **78**
- Cluster, Größe **15**
- Collector-Gruppen, Adapterinstanzen **83**

D

- Daten-Collector, Teilnehmen **86**
- Datenknoten, erstellen **24**
- Datenquellen, Verbinden **35**
- Deinstallieren von Agenten **74**

E

- Eigenschaften
 - agent.keystore.password **58**
 - agent.keystore.path **58**
 - agent.logDir **59**
 - agent.logFile **59**
 - agent.logLevel **59**
 - agent.logLevel.SystemErr **59**
 - agent.logLevel.SystemOut **59**
 - agent.proxyHost **60**
 - agent.proxyPort **60**
 - agent.setup.acceptUnverifiedCertificate **60**
 - agent.setup.camIP **60**

- agent.setup.camLogin **61**
- agent.setup.camPort **61**
- agent.setup.camPword **61**
- agent.setup.camSSLPort **62**
- agent.setup.unidirectional **62**
- agent.startupTimeOut **62**
- Agenten konfigurieren **49**
- autoinventory.defaultScan.interval.millis **63**
- autoinventory.runtimeScan.interval.millis **63**
- http.useragent **63**
- log4j **63**
- platform.log_track.eventfmt **64**
- plugins.exclude **65**
- plugins.include **66**
- postgresql.database.name.format **66**
- postgresql.index.name.format **66**
- postgresql.server.name.format **67**
- postgresql.table.name.format **67**
- scheduleThread.cancelTimeout **68**
- scheduleThread.fetchLogTimeout **68**
- scheduleThread.poolsize **68**
- scheduleThread.queueSize **69**
- snmpTrapReceiver.listenAddress **69**
- Werte verschlüsseln **54**
- End Point Operations Management **39**
- Endpoint Operations Manager-Agent, Installation und Bereitstellung **39**
- EP Ops-Agent, Installation und Bereitstellung **39**

G

- Glossar **5**
- Größe, Cluster **15**

H

- HA **27, 28**
- High Availability **27**
- Hochverfügbarkeit **28**
- hohe Verfügbarkeit **27**

I

- Installation
 - Agent **40**
 - Agenten in Eigenschaftsdatei konfigurieren **49**
 - Agenteninstallationsprogramm **40**
 - des Agenten aus einem Archiv **43, 44**
 - des Agenten aus RPM **41**
 - des Agenten mit dem Windows-Installationsprogramm **44, 46**
 - Nach der Installation **85**
 - Neu **33**
 - Neue Bereitstellung **33**
 - Vorbereiten **7**

IPv6 **14**

J

- Java-Voraussetzungen für den Agenten **47**
- JREs, Speicherorte konfigurieren **47**

K

- Keystore, konfigurieren **52**
- Klonen virtueller Maschinen, Agenten verwalten **72**
- Knoten
 - Allgemeine Anforderungen **10**
 - Best Practices **13**
 - Daten **23**
 - Master **21**
 - Netzwerkanforderungen **12**
 - Remote Collector **31**
 - Replik **27**
- Kommunikation
 - CA-Zertifikat **70**
 - sichern **70**
 - SSL **70**
 - thumbprint **70**
- Kommunikationseigenschaften, Aktivieren **50**
- Konfiguration
 - des Agenten mit dem Konfigurationsdialog **52**
 - fehlende Parameter für Objekte **80**

L

- Linux-Plattform, Agent installieren **41, 43**
- Loopback-Adresselocalhost **48**
- Lösung, vCenter Server **35**
- Lösungen, vCenter Server **37**
- Lösungsadapter, Anmeldedaten **82**

M

- Management Pack **81**
- Master-Knoten, erstellen **21**
- mehrere Agenten
 - einzeln installieren **76**
 - gleichzeitig installieren **75, 77**
 - standardmäßige Profildatei erstellen **76**
- Migration **83**

N

- Nach der Installation **85**
- Neue Bereitstellung, Installation **33**
- Neuinstallation **33**
- Neuinstallieren von Agenten **75**
- node
 - Daten **10, 23, 24**
 - Master **10, 21**
 - Remote Collector **10, 31**
 - Replik **10**

Replikat **28**
 Überblick **10**

O

Objekte
 BS-Objekte erstellen **79**
 fehlende Konfigurationsparameter **80**

P

Parameter, fehlt für Objekte **80**
 Plattformen
 Linux **41, 43**
 Windows **44, 46**
 Programm zur Verbesserung der Kundenzufriedenheit
 Teilnehmen **86**
 Verlassen **86**

R

Realize Operations Manager, Agentenvoraussetzungen **40**
 Remote Collector-Knoten erstellen **31**
 Remote-Collector-Knoten **31**
 Replikationsknoten, erstellen **28**
 Rollen **78**

S

Software aktualisieren **89**
 Software-Update **89**
 SSL, konfigurieren **70**
 Systemanforderungen, Hyperic **40**

U

Überprüfen, Zertifikate **19**
 Überschreiben von Eigenschaften für Agenten **53**
 Unterstützte Konfigurationen, Hyperic **40**

V

vCenter Server
 Lösung **35**
 Lösungen **37**
 vCenter Server-Aktionen, Benutzerzugriff **38**
 vCenter-Adapter, Instanz hinzufügen **37**
 Verbinden, Datenquellen **35**
 Verschieben von virtuellen Maschinen zwischen vCenter Servers **72**
 Virtuelle Maschine, klonen **72**
 virtuelle Maschinen, Zuordnen zu Betriebssystemen **81**
 vMotion, Löschen von virtuellen Maschinen in vRealize Operations Manager **72**
 Vor der Installation **7**

Voraussetzungen

 Installation des Realize Operations Manager **40**
 Java für den Agenten **47**
 vRealize Operations Manager, Installation **40**
 vSphere, Lösung **35**

W

Windows-Plattform
 Agent installieren **44**
 Agenten unbeaufsichtigt installieren **46**

Z

Zertifikate
 Anforderungen **16**
 Beispielinhalt **17**
 Benutzerdefiniert **16**
 Überprüfen **19**
 Zielgruppe **5**
 zuordnen, virtuelle Maschinen zu Betriebssystemen **81**

