

Sichere Konfiguration

vRealize Operations Manager 6.5

Dieses Dokument unterstützt die aufgeführten Produktversionen sowie alle folgenden Versionen, bis das Dokument durch eine neue Auflage ersetzt wird. Die neuesten Versionen dieses Dokuments finden Sie unter <http://www.vmware.com/de/support/pubs>.

DE-002407-01

vmware[®]

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

<http://www.vmware.com/de/support/>

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

- Sichere Konfiguration 5
- 1 vRealize Operations Manager -Sicherheitsaufstellung 7**
- 2 Sichere Bereitstellung von vRealize Operations Manager 9**
 - Integrität der Installationsmedien überprüfen 9
 - Härten der bereitgestellten Softwareinfrastruktur 9
 - Überprüfen installierter und nicht unterstützter Software 10
 - VMware Sicherheitsratgeber und Patches 11
- 3 Sichere Konfiguration von vRealize Operations Manager 13**
 - Sichern der vRealize Operations Manager -Konsole 14
 - Ändern des Root-Kennworts 14
 - Verwalten von Secure Shell, Administratorkonten und Konsolenzugriff 15
 - Boot Loader-Authentifizierung festlegen 20
 - Einzelnutzer- oder Wartungsmodus-Authentifizierung 20
 - Minimal erforderliche Benutzerkonten überwachen 21
 - Minimal erforderliche Gruppen überwachen 21
 - Zurücksetzen des vRealize Operations Manager -Administrator Kennworts (Linux) 22
 - NTP für VMware Appliances konfigurieren 22
 - TCP Zeitstempel-Response auf Linux deaktivieren 23
 - FIPS 140-2 Modus aktivieren 23
 - TLS für Daten während der Übertragung 24
 - Anwendungsressourcen, die geschützt werden müssen 27
 - PostgreSQL-Client-Authentifizierung konfigurieren 28
 - Apache-Konfiguration 29
 - Konfigurationsmodi deaktivieren 30
 - Verwalten unwichtiger Softwarekomponenten 30
 - Auf Linux installierte Bereitstellung 34
 - Endpoint Operations Management -Agent 35
 - Zusätzliche Aktivitäten für eine sichere Konfiguration 41
- 4 Netzwerksicherheit und sichere Kommunikation 43**
 - Netzwerkeinstellungen für Virtual Application Installation konfigurieren 43
 - Ports und Protokolle konfigurieren 52
- 5 Überwachung und Protokollierung auf Ihrem vRealize Operations Manager - System 55**
 - Sichern des Remote Logging-Servers 55
 - Autorisierten NTP-Server verwenden 55
 - Überlegungen zum Client-Browser 56

Index 57

Sichere Konfiguration

Die Dokumentation für *Sicher Konfiguration* dient als sichere Grundlage für die Bereitstellung von vRealize Operations Manager. Nutzen Sie dieses Dokument, wenn Sie Systemüberwachungs-Tools verwenden, um sicherzustellen, dass die sichere Grundlagenkonfiguration kontinuierlich hinsichtlich unerwarteter Änderungen überwacht und gewartet wird.

Hardening-Aktivitäten, die nicht schon standardmäßig eingestellt sind, können manuell ausgeführt werden.

Zielgruppe

Diese Informationen richten sich an Administratoren von vRealize Operations Manager.

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>.

vRealize Operations Manager - Sicherheitsaufstellung

1

Die Sicherheitsaufstellung von vRealize Operations Manager geht von einer vollständig sicheren Umgebung basierend auf System- und Netzwerkkonfiguration, Sicherheitsrichtlinien und Best Practices des Unternehmens aus. Es ist wichtig, dass Sie die Abhärtungsaktivitäten entsprechend den Sicherheitsrichtlinien und Best Practices Ihres Unternehmens durchführen.

Das Dokument ist in die folgenden Abschnitte unterteilt:

- Sichere Bereitstellung
- Sichere Konfiguration
- Netzwerksicherheit
- Kommunikation

Die Anleitung legt die Installation der virtuellen Applikation dar. Es wird auch der folgende Bereitstellungs-
typ besprochen:

- [„Auf Linux installierte Bereitstellung“](#), auf Seite 34

Um sicherzustellen, dass Ihr System sicher abgehärtet ist, prüfen Sie die Empfehlungen und bewerten Sie sie anhand der Sicherheitsrichtlinien und Risikobewertung Ihres Unternehmens.

Sichere Bereitstellung von vRealize Operations Manager

2

Sie müssen die Integrität der Installationsmedien überprüfen, bevor Sie das Produkt installieren, um die Authentizität der heruntergeladenen Dateien zu gewährleisten.

Dieses Kapitel behandelt die folgenden Themen:

- „Integrität der Installationsmedien überprüfen“, auf Seite 9
- „Härten der bereitgestellten Softwareinfrastruktur“, auf Seite 9
- „Überprüfen installierter und nicht unterstützter Software“, auf Seite 10
- „VMware Sicherheitsratgeber und Patches“, auf Seite 11

Integrität der Installationsmedien überprüfen

Nachdem Sie die Medien heruntergeladen haben, verwenden Sie den MD5/SHA1-Summenwert, um die Integrität des Downloads zu überprüfen. Überprüfen Sie immer den SHA1-Hash, nachdem Sie eine ISO-Datei, ein Offline-Paket oder einen Patch heruntergeladen haben, um die Integrität und Authentizität der heruntergeladenen Dateien zu gewährleisten. Wenn Sie physische Medien von VMware erwerben und das Sicherheitssiegel beschädigt ist, lassen Sie die Software von VMware austauschen.

Vorgehensweise

- ◆ Vergleichen Sie die MD5/SHA1-Hash-Ausgabe mit dem Wert, der auf der VMware Website angegeben ist.

Der SHA1 oder MD5-Hashwert müssen übereinstimmen.

HINWEIS Die vRealize Operations Manager 6.x.x.pak-Dateien sind mit dem VMware Software-Publishing-Zertifikat signiert. vRealize Operations Manager überprüft vor der Installation die Signatur der PAK-Datei.

Härten der bereitgestellten Softwareinfrastruktur

Im Rahmen der Härtung müssen Sie die bereitgestellte Softwareinfrastruktur, die Ihr VMware-System unterstützt, härten.

Bevor Sie Ihr VMware-System härten, prüfen und beheben Sie Sicherheitsdefizite in Ihrer unterstützenden Softwareinfrastruktur, um eine vollständige gehärtete und sichere Umgebung zu schaffen. Zu berücksichtigende Softwareinfrastrukturelemente umfassen Betriebssystemkomponenten, unterstützende Software und Datenbanksoftware. Beheben Sie Sicherheitsbedenken in diesen und anderen Komponenten entsprechend den Empfehlungen des Herstellers und anderen relevanten Sicherheitsprotokollen.

Härten der VMware vSphere -Umgebung

vRealize Operations Manager erfordert eine sichere VMware vSphere-Umgebung, um die größtmöglichen Vorteile und eine sichere Infrastruktur zu erreichen.

Beurteilen Sie die VMware vSphere-Umgebung, und überprüfen Sie, ob ein angemessener Grad an vSphere-Härtung durchgesetzt und aufrecht erhalten wird.

Weitere Anleitungen zum Härten finden Sie unter <http://www.vmware.com/security/hardening-guides.html>.

Härten der Linux-Installation

Lesen Sie sich die Empfehlungen in den entsprechenden Best Practice-Richtlinien für das Härten und Sichern von Linux durch, und stellen Sie sicher, dass Ihre Linux-Hosts dementsprechend gehärtet sind. Wenn Sie die Härtungsempfehlungen nicht befolgen, kann das System bekannten Sicherheitsrisiken von unsicheren Komponenten in Linux-Versionen ausgesetzt sein.

vRealize Operations Manager unterstützt die Installation auf Red Hat Enterprise Linux (RHEL) 6 ab Version 6.5.

Überprüfen installierter und nicht unterstützter Software

Schwachstellen in nicht verwendeter Software können das Risiko eines nicht autorisierten Systemzugriffs erhöhen und die Verfügbarkeit beeinträchtigen. Überprüfen Sie die auf den VMware-Host-Maschinen installierte Software und bewerten Sie ihre Verwendung.

Installieren Sie nur Software auf den vRealize Operations Manager-Knoten-Hosts, die für den sicheren Betrieb des Systems nicht erforderlich ist. Deinstallieren Sie nicht verwendete oder nicht erforderliche Software.

Das Installieren nicht unterstützter, nicht getesteter oder nicht zugelassener Software auf Infrastrukturprodukten wie vRealize Operations Manager stellt eine Bedrohung für die Infrastruktur dar.

Um die Bedrohung der Infrastruktur zu minimieren, installieren oder verwenden Sie keine Drittanbietersoftware, die von VMware nicht auf Hosts unterstützt wird, die von VMware bereitgestellt werden.

Beurteilen Sie Ihre vRealize Operations Manager-Bereitstellung und den Bestand der installierten Produkte, um zu überprüfen, ob nicht unterstützte Software installiert ist.

Weitere Informationen zu den Supportrichtlinien für Produkte von Drittanbietern finden Sie im VMware-Support auf <http://www.vmware.com/security/hardening-guides.html>.

Drittanbietersoftware überprüfen

Verwenden Sie keine Drittanbietersoftware, die nicht von VMware unterstützt wird. Überprüfen Sie, dass jegliche Drittanbietersoftware gemäß den Richtlinien des Drittanbieters sicher konfiguriert und gepatcht ist.

Nicht authentische, unsichere oder nicht behobene Schwachstellen von Drittanbietersoftware, die auf VMware Host-Maschinen installiert ist, können ein Risiko für nicht autorisierten Zugriff auf den System darstellen und die Verfügbarkeit beeinträchtigen. Jegliche Software, die nicht von VMware bereitgestellt wird, muss entsprechend gesichert und gepatcht werden.

Wenn Sie Drittanbietersoftware verwenden müssen, die nicht von VMware unterstützt wird, wenden Sie sich hinsichtlich einer sicheren Konfiguration und Patching-Anforderungen an den Drittanbieter.

VMware Sicherheitsratgeber und Patches

VMware veröffentlicht gelegentlich Sicherheitsratgeber für Produkte. Wenn Sie die Ratgeber kennen, können Sie sicherstellen, dass Sie das sicherste zugrunde liegende Produkt verwenden und dass das Produkt nicht anfällig für bekannte Bedrohungen ist.

Bewerten Sie die vRealize Operations Manager-Installation, -Patches und Aktualisierungen und überprüfen Sie, ob die veröffentlichten VMware Sicherheitsratgeber befolgt und durchgesetzt werden.

Wir empfehlen Ihnen, stets die aktuellste vRealize Operations Manager-Version zu verwenden, da diese auch die aktuellen Sicherheitskorrekturen enthält.

Weitere Informationen über die aktuellen VMware Sicherheitsratgeber finden Sie unter <http://www.vmware.com/security/advisories/>.

Sichere Konfiguration von vRealize Operations Manager

3

Als Best Practice für die Sicherheit müssen Sie die vRealize Operations Manager-Konsole sichern und Secure Shell (SSH), Administratorkonten und den Konsolenzugriff verwalten. Stellen Sie sicher, dass Ihr System mit sicheren Übertragungskanälen bereitgestellt wird.

Außerdem müssen Sie bei der Ausführung von Endpoint Operations Management-Agenten bestimmte Best Practices für die Sicherheit befolgen.

Dieses Kapitel behandelt die folgenden Themen:

- [„Sichern der vRealize Operations Manager-Konsole“](#), auf Seite 14
- [„Ändern des Root-Kennworts“](#), auf Seite 14
- [„Verwalten von Secure Shell, Administratorkonten und Konsolenzugriff“](#), auf Seite 15
- [„Boot Loader-Authentifizierung festlegen“](#), auf Seite 20
- [„Einzelnutzer- oder Wartungsmodus-Authentifizierung“](#), auf Seite 20
- [„Minimal erforderliche Benutzerkonten überwachen“](#), auf Seite 21
- [„Minimal erforderliche Gruppen überwachen“](#), auf Seite 21
- [„Zurücksetzen des vRealize Operations Manager-Administratorkennworts \(Linux\)“](#), auf Seite 22
- [„NTP für VMware Appliances konfigurieren“](#), auf Seite 22
- [„TCP Zeitstempel-Response auf Linux deaktivieren“](#), auf Seite 23
- [„FIPS 140-2 Modus aktivieren“](#), auf Seite 23
- [„TLS für Daten während der Übertragung“](#), auf Seite 24
- [„Anwendungsressourcen, die geschützt werden müssen“](#), auf Seite 27
- [„PostgreSQL-Client-Authentifizierung konfigurieren“](#), auf Seite 28
- [„Apache-Konfiguration“](#), auf Seite 29
- [„Konfigurationsmodi deaktivieren“](#), auf Seite 30
- [„Verwalten unwichtiger Softwarekomponenten“](#), auf Seite 30
- [„Auf Linux installierte Bereitstellung“](#), auf Seite 34
- [„Endpoint Operations Management-Agent“](#), auf Seite 35
- [„Zusätzliche Aktivitäten für eine sichere Konfiguration“](#), auf Seite 41

Sichern der vRealize Operations Manager -Konsole

Nachdem Sie vRealize Operations Manager installiert haben, müssen Sie sich zum ersten Mal anmelden und die Konsole jedes Knotens im Cluster sichern.

Voraussetzungen

Installieren Sie vRealize Operations Manager.

Vorgehensweise

- 1 Suchen Sie die Knotenkonsole in vCenter oder durch direkten Zugriff.
Drücken Sie in vCenter Alt+F1, um auf die Anmeldeaufforderung zuzugreifen. Aus Sicherheitsgründen sind die Remote-Sitzungen des Terminals in vRealize Operations Manager standardmäßig deaktiviert.
- 2 Melden Sie sich als „root“ an.
vRealize Operations Manager erlaubt den Zugriff auf die Befehlseingabe erst, nachdem Sie ein root-Kennwort erstellt haben.
- 3 Drücken Sie **Eingabetaste**, wenn Sie aufgefordert werden, das Kennwort einzugeben.
- 4 Drücken Sie die **Eingabetaste**, wenn Sie aufgefordert werden, das alte Kennwort einzugeben.
- 5 Wenn Sie zur Eingabe des neuen Kennworts aufgefordert werden, geben Sie das gewünschte root-Kennwort ein und notieren Sie es sich zur späteren Verwendung.
- 6 Geben Sie das root-Kennwort erneut ein.
- 7 Melden Sie bei der Konsole ab.

Ändern des Root-Kennworts

Sie können das Root-Kennwort jederzeit für alle vRealize Operations Manager-Master- oder Datenknoten über die Konsole ändern.

Der Root-Benutzer umgeht die Kennwortkomplexitätsprüfung des pam_cracklib-Moduls in `etc/pam.d/common-password`. Alle abgehärteten Appliances aktivieren `enforce_for_root` für das `pw_history`-Modul in der Datei `etc/pam.d/common-password`. Das System speichert die letzten fünf Kennwörter standardmäßig. Alte Kennwörter werden für jeden Benutzer in der Datei `/etc/security/opasswd` gespeichert.

Voraussetzungen

Überprüfen Sie, ob das Root-Kennwort für die Appliance die Anforderungen an die Komplexität von Kennwörtern Ihres Unternehmens erfüllt. Wenn das Kontokennwort mit `6` beginnt, wird ein sha512-Hash verwendet. Das ist der Standard-Hash für alle abgehärteten Appliances.

Vorgehensweise

- 1 Führen Sie den Befehl `# passwd` an der Root Shell der Appliance aus.
- 2 Um den Hash des Root-Kennworts zu überprüfen, melden Sie sich als Root an und führen Sie den Befehl `# more /etc/shadow` aus.
Die Hash-Informationen werden angezeigt.
- 3 Wenn das Root-Kennwort keinen sha512-Hash enthält, führen Sie zum Ändern den Befehl `passwd` aus.

Kennwortablauf verwalten

Konfigurieren Sie den Ablauf aller Kennwörter gemäß den Sicherheitsrichtlinien Ihres Unternehmens.

Alle abgehärteten VMware-Appliances haben standardmäßig einen Kennwortablauf von 60 Tagen. Auf den meisten abgehärteten Appliances ist für das Root-Kennwort ein Kennwortablauf von 365 Tagen festgelegt. Überprüfen Sie als Best Practice, ob der Ablauf bei allen Konten die Sicherheits- und Betriebsanforderungen erfüllt.

Wenn das Root-Kennwort abläuft, können Sie es nicht wieder einsetzen. Sie müssen standortspezifische Richtlinien implementieren, um zu verhindern, dass Administrator- und Root-Kennwörter ablaufen.

Vorgehensweise

- 1 Melden Sie sich bei Ihren virtuellen Maschinen als Root an und führen Sie den Befehl `# more /etc/shadow` aus, um den Kennwortablauf für alle Konten zu überprüfen.
- 2 Um den Ablauf für das Root-Konto zu ändern, führen Sie den Befehl `# passwd -x 365 root` aus.

In diesem Befehl steht 365 für die Anzahl der Tage bis zu Ablauf des Kennworts. Verwenden Sie denselben Befehl, um einen Benutzer zu ändern, indem Sie das spezielle Konto für root und die Anzahl der Tage ersetzen, um die Ablaufstandards Ihres Unternehmens zu erfüllen.

Das Root-Kennwort ist standardmäßig für 365 Tage festgelegt.

Verwalten von Secure Shell, Administratorkonten und Konsolenzugriff

Für Remote-Verbindungen umfassen alle abgehärteten Appliances das Secure Shell-Protokoll (SSH). SSH ist auf der abgehärteten Appliance standardmäßig deaktiviert.

SSH ist eine interaktive Befehlszeilenumgebung, die Remote-Verbindungen zu einem vRealize Operations Manager-Knoten unterstützt. SSH erfordert Anmeldeinformationen von einem Benutzerkonto mit weitreichenden Berechtigungen. SSH-Aktivitäten umgehen im Allgemeinen die rollenbasierte Zugriffskontrolle (Role-based Access Control, RBAC) und Auditkontrollen des vRealize Operations Manager-Knotens.

Deaktivieren Sie SSH in einer Produktionsumgebung als Best Practice und aktivieren Sie sie nur für die Diagnose und Fehlerbehebung bei Problemen, die nicht anderweitig behoben werden können. Lassen Sie sie nur bei Bedarf, für einen bestimmten Zweck und entsprechend den Sicherheitsrichtlinien Ihres Unternehmens aktiviert. Wenn Sie SSH aktivieren, stellen Sie sicher, dass sie vor Angriffen geschützt ist und dass Sie sie nur solange wie erforderlich aktivieren. Abhängig von Ihrer vSphere-Konfiguration können Sie SSH aktivieren oder deaktivieren, wenn Sie Ihre Open Virtualization Format-Vorlage (OVF-Vorlage) bereitstellen.

Als einfacher Test, um zu bestimmen, ob SSH auf einer Maschine aktiviert ist, versuchen Sie, eine Verbindung mit SSH zu öffnen. Wenn Sie Verbindung geöffnet wird und Anmeldeinformationen abfragt, dann ist SSH aktiviert und steht für die Herstellung von Verbindungen zur Verfügung.

Secure Shell-Root-Benutzer

Da VMware-Appliances keine vorkonfigurierten, standardmäßigen Benutzerkonten enthalten, kann das Root-Konto standardmäßig SSH verwenden, um sich direkt anzumelden. Deaktivieren Sie SSH so schnell wie möglich als Root.

Um die Compliance-Standards für Nachweisführung zu erfüllen, ist der SSH-Server auf allen abgehärteten Appliances mit dem Radeintrag `AllowGroups` vorkonfiguriert, um den SSH-Zugriff auf das sekundäre Gruppenrad einzuschränken. Um die Aufgaben zu trennen, können Sie den Radeintrag `AllowGroups` in der Datei `/etc/ssh/sshd_config` anpassen, um eine andere Gruppe wie `sshd` zu verwenden.

Die Radgruppe ist mit dem `pam_wheel`-Modul für Superbenutzerzugriff aktiviert, sodass Mitglieder der Radgruppe den `su-root`-Befehl verwenden können, für den das Root-Kennwort erforderlich ist. Durch die Trennung von Gruppen können Benutzer SSH für die Appliance nutzen, jedoch nicht den `su`-Befehl, um sich als Root anzumelden. Entfernen oder ändern Sie keine anderen Einträge im Feld `AllowGroups`, um die korrekte Funktion der Appliance sicherzustellen. Nachdem Sie die Änderungen vorgenommen haben, starten Sie den SSH-Daemon neu, indem Sie den Befehl `# service sshd restart` ausführen.

Secure Shell auf einem vRealize Operations Manager -Knoten aktivieren oder deaktivieren

Sie können Secure Shell (SSH) zur Fehlerbehebung auf einem vRealize Operations Manager-Knoten aktivieren. Um zum Beispiel die Fehlerbehebung auf einem Server durchzuführen, ist unter Umständen der Konsolenzugriff auf den Server erforderlich. Dieser erfolgt über SSH. Deaktivieren Sie SSH auf einem vRealize Operations Manager-Knoten für den normalen Betrieb.

Vorgehensweise

- 1 Greifen Sie auf die Konsole des vRealize Operations Manager-Knotens über vCenter zu.
- 2 Drücken Sie `Alt + F1`, um die Anmeldeaufforderung aufzurufen, und melden Sie sich an.
- 3 Führen Sie den Befehl `#chkconfig` aus.
- 4 Wenn der `sshd`-Dienst deaktiviert ist, führen Sie den Befehl `#chkconfig sshd on` aus.
- 5 Führen Sie den `#service sshd start`-Befehl aus, um den `sshd`-Dienst zu starten.
- 6 Führen Sie den `#service sshd stop`-Befehl aus, um den `sshd`-Dienst anzuhalten.

Ein lokales Administratorkonto für Secure Shell erstellen

Sie müssen lokale Administratorkonten erstellen, die sowohl als Secure Shell (SSH) verwendet werden können und die Mitglieder der sekundären `Wheel`-Gruppe sind, bevor Sie den Root-SSH-Zugriff entfernen.

Bevor Sie den direkten Root-Zugriff deaktivieren, testen Sie mit `AllowGroups`, ob autorisierte Administratoren auf SSH zugreifen können und dass sie die `Wheel`-Gruppe nutzen und den Befehl `su` verwenden können, um sich als Root anzumelden.

Vorgehensweise

- 1 Melden Sie sich als Root an, und führen Sie die folgenden Befehle aus.

```
# useradd -d /home/vropsuser -g users -G wheel -m
# passwd username
```

`Wheel` ist die Gruppe, die in `AllowGroups` für SSH-Zugriff festgelegt wurde. Um mehrere sekundäre Gruppen hinzuzufügen, verwenden Sie `-G wheel, sshd`.

- 2 Wechseln Sie zum Benutzer, und stellen Sie ein neues Kennwort bereit, um eine Prüfung der Kennwortkomplexität zu gewährleisten.

```
# su - username
username@hostname:~>passwd
```

Bei Erfüllung der Kennwortkomplexität wird das Kennwort aktualisiert. Wenn die Kennwortkomplexität nicht erfüllt wird, wird wieder das ursprüngliche Kennwort verwendet, und Sie müssen den Kennwortbefehl erneut ausführen.

Nachdem Sie die Anmeldekonto erstellt haben, um Remote-SSH-Zugriff zu ermöglichen, und den Befehl `su` für die Anmeldung als Root mit `Wheel`-Zugriff verwendet haben, können Sie das Root-Konto aus der SSH-Direktanmeldung entfernen.

- Um Direktanmeldung bei SSH zu entfernen, ändern Sie die Datei `/etc/ssh/sshd_config`, indem Sie `(#)PermitRootLogin yes` durch `PermitRootLogin no` ersetzen.

Weiter

Deaktivieren Sie Direktanmeldungen als Root. Standardmäßig erlauben die gehärteten Appliances die direkte Anmeldung als Root über die Konsole. Nachdem Sie Administratorkonten für NonRepudiation erstellt und sie auf Wheel-Zugriff (`su-root`) getestet haben, deaktivieren Sie direkte Root-Anmeldungen, indem Sie die Datei `/etc/security` als Root bearbeiten und den Eintrag `tty1` durch `console` ersetzen.

Secure Shell-Zugriff einschränken

Schränken Sie im Rahmen Ihres Systemabhärtungsprozesses den Secure Shell-Zugriff (SSH-Zugriff) ein, indem Sie das Paket `tcp_wrappers` auf allen Host-Maschinen der virtuellen VMware-Appliance entsprechend konfigurieren. Erhalten Sie auch die erforderlichen SSH-Schlüsseldateiberechtigungen auf diesen Appliances aufrecht.

Alle virtuellen VMware-Appliances enthalten das Paket `tcp_wrappers`, damit TCP-gestützte Daemons die Netzwerk-Subnetze steuern können, die auf die Libwrapped-Daemons zugreifen. Die Datei `/etc/hosts.allow` enthält standardmäßig einen generischen Eintrag, `sshd: ALL : ALLOW`, der jeglichen Zugriff auf die Secure Shell zulässt. Schränken Sie den Zugriff entsprechend den Anforderungen Ihres Unternehmens ein.

Vorgehensweise

- Öffnen Sie die Datei `/etc/hosts.allow` auf der Host-Maschine Ihrer virtuellen Appliance in einem Texteditor.
- Ändern Sie den generischen Eintrag in Ihrer Produktionsumgebung so, dass er nur die lokalen Host-Einträge und das Subnetz des Managementnetzwerks enthält, um einen sicheren Betrieb zu gewährleisten.

```
sshd:127.0.0.1 : ALLOW
sshd: [::1] : ALLOW
sshd: 10.0.0.0 :ALLOW
```

In diesem Beispiel sind alle lokalen Host-Verbindungen und Verbindungen erlaubt, die Clients auf dem Subnetz 10.0.0.0 herstellen.

- Fügen Sie die erforderliche Maschinenidentifikation hinzu, zum Beispiel Hostname, IP-Adresse, vollständig qualifizierter Domänenname (FQDN) und Loopback.
- Speichern und schließen Sie die Datei.

Secure Shell-Schlüsseldateiberechtigungen aufrecht erhalten

Um einen angemessenen Grad an Sicherheit aufrecht zu erhalten, konfigurieren Sie Secure Shell- (SSH-) Schlüsseldateiberechtigungen.

Vorgehensweise

- Sehen Sie sich die Public Host-Schlüsseldateien in `/etc/ssh/*key.pub` an.
- Überprüfen Sie, ob diese Dateien im Besitz von Root sind, ob die Gruppe im Besitz von Root ist und ob die Dateien Berechtigungen haben, die auf 0644 festgelegt sind.

Die Berechtigungen sind `(-rw-r--r--)`.

- Schließen Sie alle Dateien.
- Sehen Sie sich die Private Host-Schlüsseldateien in `/etc/ssh/*key.pub` an.

- 5 Überprüfen Sie, ob diese Dateien und die Gruppe im Besitz von Root sind und ob die Dateien Berechtigungen haben, die auf 0600 festgelegt sind.
Die Berechtigungen sind (-rw-----).
- 6 Schließen Sie alle Dateien.

Härten der Secure Shell-Serverkonfiguration

Wenn möglich, verfügt die Virtual Application Installation (OVF) über eine standardmäßig gehärtete Konfiguration. Benutzer können überprüfen, ob ihre Konfiguration entsprechend gehärtet ist, indem Sie den Server- und Client-Dienst im Abschnitt mit globalen Optionen der Konfigurationsdatei untersuchen.

Falls möglich, beschränken Sie den SSH-Server in der Datei `/etc/hosts.allow` auf ein Verwaltungsunternetz.

Vorgehensweise

- 1 Öffnen Sie die Serverkonfigurationsdatei `/etc/ssh/sshd_config`, und überprüfen Sie, ob die Einstellungen korrekt sind.

Einstellung	Status
Server-Daemonprotokoll	Protocol 2
Verschlüsselungen	Verschlüsselungen aes256-ctr,aes128-ctr
TCP-Weiterleitung	AllowTCPForwarding nein
Server Gateway-Ports	Gateway-Ports nein
X11-Weiterleitung	X11Forwarding nein
SSH-Dienst	Verwenden Sie das Feld „AllowGroups“, um eine Gruppe festzulegen, für die der Zugriff erlaubt ist, und fügen Sie Mitglieder zur sekundären Gruppe der Benutzer hinzu, die den Dienst verwenden dürfen.
GSSAPI-Authentifizierung	GSSAPIAuthentication nein, sofern nicht verwendet
Kerberos-Authentifizierung	KerberosAuthentication ein, sofern nicht verwendet
Lokale Variablen (globale AcceptEnv-Option)	Auf deaktiviert durch Auskommentieren oder nur für LC_* oder LANG Variablen aktiviert festlegen
Tunnel-Konfiguration	PermitTunnel nein
Netzwerksitzungen	MaxSessions 1
Strikte Modusüberprüfung	Strikte Modi ja
Berechtigungstrennung	UsePrivilegeSeparation ja
rhosts RSA-Authentifizierung	RhostsRSAAuthentication nein
Komprimierung	Komprimierung verzögert oder Komprimierung nein
Meldungsauthentifizierungscode	MACs hmac-sha1
Benutzerzugriffseinschränkung	PermitUserEnvironment nein

- 2 Speichern Sie die Änderungen, und schließen Sie die Datei.

Härten der Secure Shell-Client-Konfiguration

Überprüfen Sie im Rahmen Ihrer Überwachung der Systemhärtung die Härtung des SSH-Clients, indem Sie die SSH-Client-Konfigurationsdatei auf den Host-Computern der virtuellen Appliances untersuchen, um sicherzustellen, dass sie entsprechend den VMware Richtlinien konfiguriert ist.

Vorgehensweise

- 1 Öffnen Sie die Konfigurationsdatei `/etc/ssh/ssh_config`, und überprüfen Sie, ob die Einstellungen im Abschnitt mit globalen Optionen korrekt sind.

Einstellung	Status
Client-Protokoll	Protocol 2
Client Gateway-Ports	Gateway-Ports nein
GSSAPI-Authentifizierung	GSSAPIAuthentication nein
Lokale Variablen (globale SendEnv-Option)	Nur LC_* oder LANG Variablen bereitstellen
CBC-Verschlüsselungen	Verschlüsselungen aes256-ctr,aes128-ctr
Meldungsauthentifizierungs-codes	Wird nur im Eintrag MACs <code>hmac-sha1</code> verwendet

- 2 Speichern Sie die Änderungen, und schließen Sie die Datei.

Direktanmeldungen als Root deaktivieren

Standardmäßig ermöglichen Ihnen die gehärteten Appliances, die Konsole so zu verwenden, dass Sie sich direkt als Root anmelden können. Als Best Practice für die Sicherheit können Sie Direktanmeldungen deaktivieren, nachdem Sie ein Administratorkonto für NonRepudiation erstellt und es mit dem Befehl `su-root` auf Wheel-Zugriff getestet haben.

Voraussetzungen

- Führen Sie die Schritte aus, die in „[Ein lokales Administratorkonto für Secure Shell erstellen](#)“, auf Seite 16 beschrieben sind.
- Verifizieren Sie, dass Sie Ihren Zugriff auf das System als Administrator getestet haben, bevor Sie Direktanmeldungen als Root deaktivieren.

Vorgehensweise

- 1 Melden Sie sich als Root an, und navigieren Sie zur Datei `/etc/security`.
Sie können auf Ebene der Eingabeaufforderung auf die Datei zugreifen.
- 2 Ersetzen Sie den Eintrag `tty1` durch `console`.

SSH-Zugriff für das Admin-Benutzerkonto deaktivieren

Um Sicherheitsvorkehrungen zu treffen, gilt es als Best Practice, für das Admin-Benutzerkonto den SSH-Zugriff zu deaktivieren. Das vRealize Operations Manager Admin-Konto und das Linux Admin-Konto benutzen dasselbe Kennwort. Die Deaktivierung des SSH-Zugriffs für den Admin-Benutzer erzwingt eine Sicherheitsstrategie mit Tiefgang, indem sich alle Benutzer von SSH erst bei einem Dienstkonto mit weniger Rechten anmelden müssen mit einem Kennwort, das sich von dem des vRealize Operations Manager Admin-Kontos unterscheidet, um danach auf ein Konto mit mehr Rechten zu wechseln, z. B. Admin oder Root.

Vorgehensweise

- 1 Bearbeiten Sie die Datei `/etc/ssh/sshd_config`.
Sie können auf Ebene der Eingabeaufforderung auf die Datei zugreifen.
- 2 Fügen Sie den Eintrag `DenyUsers admin` an beliebiger Stelle in die Datei ein und speichern Sie dann die Datei.
- 3 Um den sshd-Server neu zu starten, führen Sie den Befehl `service sshd restart` aus.

Boot Loader-Authentifizierung festlegen

Um einen angemessenen Grad an Sicherheit bereitzustellen, konfigurieren Sie die Boot Loader-Authentifizierung auf Ihren virtuellen VMware-Appliances. Wenn der Boot Loader des Systems keine Authentifizierung erfordert, könnten Benutzer mit Konsolenzugriff auf das System die Boot-Konfiguration des Systems ändern oder das System im Einzelnutzer- oder Wartungsmodus starten, was zu Denial-of-Service oder nicht autorisiertem Systemzugriff führen kann.

Da die Boot Loader-Authentifizierung auf den virtuellen VMware-Appliances nicht standardmäßig festgelegt ist, müssen Sie für die Konfiguration ein GRUB-Kennwort erstellen.

Vorgehensweise

- 1 Überprüfen Sie, ob ein Boot-Kennwort vorhanden ist, indem Sie die Zeile `password --md5 <password-hash>` in der Datei `/boot/grub/menu.lst` auf Ihrer virtuellen Appliance suchen.
- 2 Wenn kein Kennwort vorhanden ist, führen Sie den Befehl `# /usr/sbin/grub-md5-crypt` auf Ihrer virtuellen Appliance aus.
Es wird ein D5-Kennwort generiert und der Befehl stellt die md5-Hash-Ausgabe bereit.
- 3 Übertragen Sie das Kennwort in die Datei `menu.lst`, indem Sie den Befehl `# password --md5 <hash from grub-md5-crypt>` ausführen.

Einzelnutzer- oder Wartungsmodus-Authentifizierung

Wenn das System keine gültige root-Authentifizierung erfordert, bevor es in den Einzelnutzer- oder Wartungsmodus bootet, erhält jeder, der den Einzelnutzer- oder Wartungsmodus aufruft, privilegierten Zugriff auf alle Dateien im System.

Vorgehensweise

- ◆ Überprüfen Sie die Datei `/etc/inittab` und stellen Sie sicher, dass die folgenden zwei Zeilen vorhanden sind: `ls:S:wait:/etc/init.d/rc S` und `~:S:respawn:/sbin/sulogin`.

Minimal erforderliche Benutzerkonten überwachen

Sie müssen vorhandene Benutzerkonten überwachen und sicherstellen, dass alle unnötigen Benutzerkonten entfernt werden.

Vorgehensweise

- ◆ Führen Sie den Befehl `host:~ # cat /etc/passwd` aus und überprüfen Sie die minimal erforderlichen Benutzerkonten:

```
bin:x:1:1:bin:/bin:/bin/bash
daemon:x:2:2:Daemon:/sbin:/bin/bash
haldaemon:x:101:102:User for haldaemon:/var/run/hald:/bin/false
mail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/false
man:x:13:62:Manual pages viewer:/var/cache/man:/bin/bash
messagebus:x:100:101:User for D-Bus:/var/run/dbus:/bin/false
nobody:x:65534:65533:nobody:/var/lib/nobody:/bin/bash
ntp:x:74:106:NTP daemon:/var/lib/ntp:/bin/false
polkituser:x:103:104:PolicyKit:/var/run/PolicyKit:/bin/false
postfix:x:51:51:Postfix Daemon:/var/spool/postfix:/bin/false
root:x:0:0:root:/root:/bin/bash
sshd:x:71:65:SSH daemon:/var/lib/ssh:/bin/false
suse-ncc:x:104:107:Novell Customer Center User:/var/lib/YaST2/suse-ncc-fakehome:/bin/bash
uidd:x:102:103:User for uidd:/var/run/uidd:/bin/false
wwwrun:x:30:8:WWW daemon apache:/var/lib/wwwrun:/bin/false
nginx:x:105:108:user for nginx:/var/lib/nginx:/bin/false
admin:x:1000:1003:~/home/admin:/bin/bash
tcserver:x:1001:1004:tc Server User:/home/tcserver:/bin/bash
postgres:x:1002:100:~/var/vmware/vpostgres/9.3:/bin/bash
```

Minimal erforderliche Gruppen überwachen

Sie müssen vorhandene Gruppen und Mitglieder überwachen, um sicherzustellen, dass alle unnötigen Gruppen oder Gruppenzugehörigkeiten entfernt werden.

Vorgehensweise

- ◆ Führen Sie den Befehl `<host>:~ # cat /etc/group` aus, um die minimal erforderlichen Gruppen und Gruppenmitgliedschaften zu überprüfen.

```
audio:x:17:
bin:x:1:daemon
cdrom:x:20:
console:x:21:
daemon:x:2:
dialout:x:16:u1,tcserver,postgres
disk:x:6:
floppy:x:19:
haldaemon:!:102:
kmem:x:9:
mail:x:12:
man:x:62:
messagebus:!:101:
modem:x:43:
nobody:x:65533:
nogroup:x:65534:nobody
ntp:!:106:
```

```

polkituser:!:105:
public:x:32:
root:x:0:admin
shadow:x:15:
sshd:!:65:
suse-ncc:!:107:
sys:x:3:
tape:!:103:
trusted:x:42:
tty:x:5:
utmp:x:22:
uidd:!:104:
video:x:33:u1,tcserver,postgres
wheel:x:10:root,admin
www:x:8:
xok:x:41:
maildrop:!:1001:
postfix:!:51:
users:x:100:
vami:!:1002:root
nginx:!:108:
admin:!:1003:
vfabric:!:1004:admin,wwwrun

```

Zurücksetzen des vRealize Operations Manager - Administratorkeywords (Linux)

Als Best Practice für die Sicherheit können Sie das vRealize Operations Manager-Kennwort auf Linux-Clustern für vApp- oder Linux-Installationen zurücksetzen.

Vorgehensweise

- 1 Melden Sie sich auf der Remote-Konsole des Master-Knotens als root-Benutzer an.
- 2 Geben Sie den Befehl `$VMWARE_PYTHON_BIN $VCOPS_BASE/./vmware-vcopssuite/utilities/sliceConfiguration/bin/vcopsSetAdminPassword.py --reset` ein und folgen Sie den Eingabeaufforderungen.

NTP für VMware Appliances konfigurieren

Deaktivieren Sie für kritisches Time-Sourcing die Host-Zeitsynchronisierung und verwenden Sie das Network Time Protocol (NTP) für VMware Appliances. Sie müssen einen vertrauenswürdigen NTP-Remoteserver für die Zeitsynchronisierung konfigurieren. Der NTP-Server muss ein autoritativer Zeitserver sein, oder er muss mindestens mit einem autoritativen Zeitserver synchronisiert sein.

Der NTP-Daemon für virtuelle VMware Appliances bietet synchronisierte Zeitdienste. NTP ist standardmäßig deaktiviert, sodass Sie es manuell konfigurieren müssen. Falls möglich, verwenden Sie NTP in Produktionsumgebungen, um Benutzeraktionen zu verfolgen und möglicherweise schadhafte Angriffe und Eindringlinge über akkurate Überwachung und Protokollierung zu erkennen. Informationen zu NTP-Sicherheitshinweisen finden Sie auf der NTP-Website.

Die NTP-Konfigurationsdatei befindet sich in der Datei `/etc/ntp.conf` auf jeder Appliance.

Vorgehensweise

- 1 Navigieren Sie zur `/etc/ntp.conf`-Konfigurationsdatei auf dem Host-Computer Ihrer virtuellen Appliance.
- 2 Legen Sie den Dateibesitzer auf `root:root` fest.

- 3 Legen Sie die Berechtigungen auf **0640** fest.
- 4 Um das Risiko eines Denial-of-Service-Verstärkungsangriffs auf den NTP-Dienst zu mindern, öffnen Sie die Datei `/etc/ntp.conf`, und stellen Sie sicher, dass die Einschränkungszeilen in der Datei vorhanden sind.

```
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict -6 ::1
```

- 5 Speichern Sie alle Änderungen, und schließen Sie die Dateien.

Informationen zu NTP-Sicherheitshinweisen finden Sie unter <http://support.ntp.org/bin/view/Main/SecurityNotice>.

TCP Zeitstempel-Response auf Linux deaktivieren

Die TCP Zeitstempel-Response wird verwendet, um die Betriebszeit des Remote-Host zu schätzen und weitere Angriffe zu unterstützen. Darüber hinaus können basierend auf dem Verhalten der TCP Zeitstempel bei einigen Betriebssystemen Fingerprints erstellt werden.

Vorgehensweise

- ◆ Deaktivieren Sie TCP Zeitstempel-Response auf Linux.
 - a Um den Wert für `net.ipv4.tcp_timestamps` auf `0` festzulegen, führen Sie den Befehl `sysctl -w net.ipv4.tcp_timestamps=0` aus.
 - b Fügen Sie den Wert `ipv4.tcp_timestamps=0` zur Standarddatei `sysctl.conf` hinzu.

FIPS 140-2 Modus aktivieren

Die Version von OpenSSL, die mit vRealize Operations Manager Version 6.3 und jünger ausgeliefert wird, ist gemäß FIPS 140-2 zertifiziert. Der FIPS-Modus ist standardmäßig jedoch nicht aktiviert.

Sie können den FIPS-Modus aktivieren, wenn es aus Gründen der Übereinstimmung mit Sicherheitsanforderungen erforderlich ist, durch Aktivierung des FIPS-Modus FIPS-zertifizierte kryptografische Algorithmen zu benutzen.

Vorgehensweise

- 1 Um die Datei `mod_ssl.so` zu ersetzen, führen Sie folgenden Befehl aus:


```
cd /usr/lib64/apache2-prefork/
cp mod_ssl.so mod_ssl.so.old
cp mod_ssl.so.FIPS0N.openssl1.0.2 mod_ssl.so
```
- 2 Ändern Sie Ihre Apache2-Konfiguration, indem Sie die Datei `/etc/apache2/ssl-global.conf` bearbeiten.
- 3 Suchen Sie nach der Zeile `<IfModule mod_ssl.c>` und fügen Sie darunter die Weisung `SSLFIPS on` hinzu.
- 4 Um die Apache-Konfiguration zurückzusetzen, führen Sie den Befehl `service apache2 restart` aus.

TLS für Daten während der Übertragung

Als Best Practice für die Sicherheit müssen Sie sicherstellen, dass das System mit sicheren Übertragungskanälen bereitgestellt wird.

Starke Protokolle für vRealize Operations Manager konfigurieren

Protokolle wie SSLv2 und SSLv3 werden nicht mehr als sicher erachtet. Außerdem wird empfohlen, TLS 1.0 zu deaktivieren. Aktivieren Sie nur TLS 1.1 und TLS 1.2.

Sicherstellen der richtigen Verwendung von Protokollen in Apache HTTPD

vRealize Operations Manager deaktiviert SSLv2 und SSLv3 standardmäßig. Sie müssen schwache Protokolle in jedem Load Balancer deaktivieren, bevor das System in einer Produktionsumgebung eingesetzt wird.

Vorgehensweise

- 1 Führen Sie in der Befehlszeile den folgenden Befehl aus, um zu überprüfen, ob SSLv2 und SSLv3 deaktiviert sind: `grep SSLProtocol /usr/lib/vmware-vcopsuite/utilities/conf/vcops-apache.conf | grep -v '#'`.

Wenn die Protokolle deaktiviert sind, gibt der Befehl die folgende Ausgabe zurück: `SSLProtocol All -SSLv2 -SSLv3`

- 2 Um auch das TLS 1.0-Protokoll zu deaktivieren, führen Sie den folgenden Befehl in der Befehlszeile aus: `sed -i "/^[^#]*SSLProtocol/ c\SSLProtocol All -SSLv2 -SSLv3 -TLSv1" /usr/lib/vmware-vcopsuite/utilities/conf/vcops-apache.conf`.
- 3 Führen Sie zum Neustarten des Apache2-Servers den folgenden Befehl in der Befehlszeile aus: `/etc/init.d/apache2 restart`.

Sicherstellen der richtigen Verwendung von Protokollen im GemFire-TLS-Handler

vRealize Operations Manager deaktiviert SSLv3 standardmäßig. Sie müssen schwache Protokolle in jedem Load Balancer deaktivieren, bevor das System in einer Produktionsumgebung eingesetzt wird.

Vorgehensweise

- 1 Überprüfen Sie, ob die Protokolle aktiviert sind. Führen Sie auf jedem Knoten die folgenden Befehle aus, um zu überprüfen, ob die Protokolle aktiviert sind:

```
grep cluster-ssl-protocol /usr/lib/vmware-vcops/user/conf/gemfire.properties | grep -v '#'
```

Das folgende Ergebnis wird erwartet:

```
cluster-ssl-protocols=TLSv1.2 TLSv1.1 TLSv1
```

```
grep cluster-ssl-protocol /usr/lib/vmware-vcops/user/conf/gemfire.native.properties | grep -v '#'
```

Das folgende Ergebnis wird erwartet:

```
cluster-ssl-protocols=TLSv1.2 TLSv1.1 TLSv1
```

```
grep cluster-ssl-protocol /usr/lib/vmware-vcops/user/conf/gemfire.locator.properties | grep -v '#'
```

Das folgende Ergebnis wird erwartet:

```
cluster-ssl-protocols=TLSv1.2 TLSv1.1 TLSv1
```


- 2 Deaktivieren Sie TLS 1.0.
 - a Navigieren Sie zur Administrator-Benutzeroberfläche unter `url/admin`.
 - b Klicken Sie auf **Offline stellen**.
 - c Führen Sie die folgenden Befehle aus, um SSLv3 und TLS 1.0 zu deaktivieren:


```
sed -i "/^[^#]*cluster-ssl-protocol/ c\cluster-ssl-protocols=TLSv1.2
TLSv1.1" /usr/lib/vmware-vcops/user/conf/gemfire.properties
sed -i "/^[^#]*cluster-ssl-protocol/ c\cluster-ssl-protocols=TLSv1.2
TLSv1.1" /usr/lib/vmware-vcops/user/conf/gemfire.native.properties
sed -i "/^[^#]*cluster-ssl-protocol/ c\cluster-ssl-protocols=TLSv1.2
TLSv1.1" /usr/lib/vmware-vcops/user/conf/gemfire.locator.properties
```

 Wiederholen Sie für jeden Knoten diesen Schritt.
 - d Navigieren Sie zur Administrator-Benutzeroberfläche.
 - e Klicken Sie auf **Online stellen**.
- 3 Aktivieren Sie TLS 1.0 wieder.
 - a Navigieren Sie zur Administrator-Benutzeroberfläche unter `url/admin`, um den Cluster offline zu stellen.
 - b Klicken Sie auf **Offline stellen**.
 - c Führen Sie die folgenden Befehle aus, um sicherzustellen, dass SSLv3 und TLS 1.0 deaktiviert sind:


```
sed -i "/^[^#]*cluster-ssl-protocol/ c\cluster-ssl-protocols=TLSv1.2 TLSv1.1
TLSv1" /usr/lib/vmware-vcops/user/conf/gemfire.properties
sed -i "/^[^#]*cluster-ssl-protocol/ c\cluster-ssl-protocols=TLSv1.2 TLSv1.1
TLSv1" /usr/lib/vmware-vcops/user/conf/gemfire.native.properties
sed -i "/^[^#]*cluster-ssl-protocol/ c\cluster-ssl-protocols=TLSv1.2 TLSv1.1
TLSv1" /usr/lib/vmware-vcops/user/conf/gemfire.locator.properties
```

 Wiederholen Sie diesen Schritt für jeden Knoten.
 - d Navigieren Sie zur Administrator-Benutzeroberfläche, um den Cluster online zu stellen.
 - e Klicken Sie auf **Online stellen**.

vRealize Operations Manager für die Verwendung starker Verschlüsselungen konfigurieren

Für maximale Sicherheit müssen Sie vRealize Operations Manager-Komponenten so konfigurieren, dass sie starke Verschlüsselungen verwenden. Um sicherzustellen, dass nur starke Verschlüsselungen ausgewählt werden, deaktivieren Sie die Verwendung schwacher Verschlüsselungen. Konfigurieren Sie den Server so, dass er nur starke Verschlüsselungen unterstützt und dass ausreichend große Schlüsselgrößen verwendet werden. Außerdem sollten die Verschlüsselungen in einer geeigneten Reihenfolge konfiguriert werden.

vRealize Operations Manager deaktiviert die Verwendung von Verschlüsselungssuites, die den DHE-Schlüsselaustausch standardmäßig verwenden. Vergewissern Sie sich, dass Sie diese schwachen Verschlüsselungssuites auf allen Lastausgleichen deaktivieren, bevor Sie das System in Produktion nehmen.

Starke Verschlüsselungen verwenden

Die Verschlüsselung, die zwischen dem Server und dem Browser ausgehandelt wird, bestimmt die Schlüsselaustauschmethode und die Verschlüsselungsstärke, die in einer TLS-Sitzung verwendet wird.

Sicherstellen der richtigen Verwendung der Cipher-Suites in Apache HTTPD

Stellen Sie die richtige Verwendung der Cipher-Suites in Apache HTTPD sicher, um für maximale Sicherheit zu sorgen.

Vorgehensweise

- 1 Führen Sie in der Befehlszeile den folgenden Befehl aus, um die richtige Verwendung der Cipher-Suites in Apache HTTPD sicherzustellen: `grep SSLCipherSuite /usr/lib/vmware-vcopsuite/utilities/conf/vcops-apache.conf | grep -v '#'`.

Wenn Apache HTTPD die richtigen Cipher-Suites verwendet, gibt der Befehl die folgende Ausgabe zurück: `SSLCipherSuite kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:!DH`

- 2 Führen Sie in der Befehlszeile den folgenden Befehl aus, um die richtige Verwendung der Cipher-Suites zu konfigurieren: `sed -i "/^[^#]*SSLCipherSuite/ c\SSLCipherSuite kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:!DH" /usr/lib/vmware-vcopsuite/utilities/conf/vcops-apache.conf`.

Führen Sie diesen Befehl aus, wenn die Ausgabe in Schritt 1 nicht Ihren Erwartungen entspricht.

Mit diesem Befehl werden alle Cipher-Suites deaktiviert, die DH- und DHE-Schlüsselaustauschmethoden verwenden.

- 3 Führen Sie in der Befehlszeile den folgenden Befehl aus, um den Apache2-Server neu zu starten: `/etc/init.d/apache2 restart`.
- 4 Um DH wieder zu aktivieren, entfernen Sie !DH aus den Cipher-Suites, indem Sie den folgenden Befehl in der Befehlszeile ausführen: `sed -i "/^[^#]*SSLCipherSuite/ c\SSLCipherSuite kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP" /usr/lib/vmware-vcopsuite/utilities/conf/vcops-apache.conf`.
- 5 Führen Sie in der Befehlszeile den folgenden Befehl aus, um den Apache2-Server neu zu starten: `/etc/init.d/apache2 restart`.

Sicherstellen der richtigen Verwendung der Cipher-Suites im GemFire-TLS-Handler

Stellen Sie die richtige Verwendung der Cipher-Suites im GemFire-TLS-Handler sicher, um für maximale Sicherheit zu sorgen.

Vorgehensweise

- 1 Führen Sie auf jedem Knoten die folgenden Befehle aus, um sicherzustellen, dass die Protokolle und somit die Cipher-Suites aktiviert sind:

```
grep cluster-ssl-ciphers /usr/lib/vmware-vcops/user/conf/gemfire.properties | grep -v '#'
```

```
grep cluster-ssl-ciphers /usr/lib/vmware-vcops/user/conf/gemfire.native.properties | grep -v '#'
```

```
grep cluster-ssl-ciphers /usr/lib/vmware-vcops/user/conf/gemfire.locator.properties | grep -v '#'
```

- 2 Konfigurieren Sie die richtigen Cipher-Suites.
 - a Navigieren Sie zur Administrator-Benutzeroberfläche unter `URL/admin`.
 - b Klicken Sie auf **Offline stellen**, um den Cluster offline zu stellen.

- c Führen Sie die folgenden Befehle aus, um die richtigen Cipher-Suites zu konfigurieren:

```
sed -i "/^[^#]*cluster-ssl-ciphers/ c\cluster-ssl-ciphers=TLS_ECD-
HE_RSA_WITH_AES_128_GCM_SHA256" /usr/lib/vmware-vcops/user/conf/gemfire.properties
```

```
sed -i "/^[^#]*cluster-ssl-ciphers/ c\cluster-ssl-ciphers=TLS_ECD-
HE_RSA_WITH_AES_128_GCM_SHA256" /usr/lib/vmware-vcops/user/conf/gemfire.native.properties
```

```
sed -i "/^[^#]*cluster-ssl-ciphers/ c\cluster-ssl-ciphers=TLS_ECD-
HE_RSA_WITH_AES_128_GCM_SHA256" /usr/lib/vmware-vcops/user/conf/gemfire.locator.properties
```

Wiederholen Sie diesen Schritt für jeden Knoten.

- d Navigieren Sie zur Administrator-Benutzeroberfläche unter *URL/admin*.
- e Klicken Sie auf **Online stellen**.

Anwendungsressourcen, die geschützt werden müssen

Stellen Sie als Best Practice für die Sicherheit sicher, dass die Anwendungsressourcen geschützt sind.

Befolgen Sie die Schritte, um sicherzustellen, dass die Anwendungsressourcen geschützt sind.

Vorgehensweise

- 1 Führen Sie den Befehl `find / -path /proc -prune -o -type f -perm +6000 -ls` aus, um zu überprüfen, ob für die Dateien ordnungsgemäß definierte SUID- und GUID-Bits festgelegt sind.

Die folgende Liste wird angezeigt:

```
354131 24 -rwsr-xr-x 1 polkituser root 23176 /usr/lib/PolicyKit/polkit-set-default-helper
354126 20 -rwxr-sr-x 1 root polkituser 19208 /usr/lib/PolicyKit/polkit-grant-helper
354125 20 -rwxr-sr-x 1 root polkituser 19008 /usr/lib/PolicyKit/polkit-explicit-grant-helper
354130 24 -rwxr-sr-x 1 root polkituser 23160 /usr/lib/PolicyKit/polkit-revoke-helper
354127 12 -rwsr-x--- 1 root polkituser 10744 /usr/lib/PolicyKit/polkit-grant-helper-pam
354128 16 -rwxr-sr-x 1 root polkituser 14856 /usr/lib/PolicyKit/polkit-read-auth-helper
73886 84 -rwsr-xr-x 1 root shadow 77848 /usr/bin/chsh
73888 88 -rwsr-xr-x 1 root shadow 85952 /usr/bin/gpasswd
73887 20 -rwsr-xr-x 1 root shadow 19320 /usr/bin/expiry
73890 84 -rwsr-xr-x 1 root root 81856 /usr/bin/passwd
73799 240 -rwsr-xr-x 1 root root 238488 /usr/bin/sudo
73889 20 -rwsr-xr-x 1 root root 19416 /usr/bin/newgrp
73884 92 -rwsr-xr-x 1 root shadow 86200 /usr/bin/chage
73885 88 -rwsr-xr-x 1 root shadow 82472 /usr/bin/chfn
73916 40 -rwsr-x--- 1 root trusted 40432 /usr/bin/crontab
296275 28 -rwsr-xr-x 1 root root 26945 /usr/lib64/pt_chown
353804 816 -r-xr-sr-x 1 root mail 829672 /usr/sbin/sendmail
278545 36 -rwsr-xr-x 1 root root 35792 /bin/ping6
278585 40 -rwsr-xr-x 1 root root 40016 /bin/su
278544 40 -rwsr-xr-x 1 root root 40048 /bin/ping
278638 72 -rwsr-xr-x 1 root root 69240 /bin/umount
278637 100 -rwsr-xr-x 1 root root 94808 /bin/mount
```

```

475333  48 -rwsr-x---  1 root    messagebus  47912 /lib64/dbus-1/dbus-daemon-launch-hel-
per
41001   36 -rwsr-xr-x   1 root    shadow      35688 /sbin/unix_chkpwd
41118   12 -rwsr-xr-x   1 root    shadow      10736 /sbin/unix2_chkpwd

```

- 2 Führen Sie den Befehl `find / -path */proc -prune -o -nouser -o -nogroup` aus, um zu überprüfen, ob alle Dateien in der vApp einen Besitzer haben.
Alle Dateien haben einen Besitzer, wenn keine Ergebnisse angezeigt werden.
- 3 Führen Sie den Befehl `find / -name "*.*" -type f -perm -a+w | xargs ls -ldb` aus, um zu überprüfen, ob die Dateien global schreibbare Dateien sind, indem Sie die Berechtigungen aller Dateien in der vApp überprüfen.
Keine der Dateien darf die Berechtigung `xx2` haben.
- 4 Führen Sie den Befehl `find / -path */proc -prune -o ! -user root -o -user admin -print` aus, um zu überprüfen, ob die Dateien im Besitz des korrekten Benutzers sind.
Alle Dateien gehören entweder `root` oder `admin`, wenn keine Ergebnisse angezeigt werden.
- 5 Führen Sie den Befehl `find /usr/lib/vmware-casa/ -type f -perm -o=w` aus, um sicherzustellen, dass die Dateien im Verzeichnis `/usr/lib/vmware-casa/` nicht global schreibbar sind.
Es dürfen keine Ergebnisse angezeigt werden.
- 6 Führen Sie den Befehl `find /usr/lib/vmware-vcops/ -type f -perm -o=w` aus, um sicherzustellen, dass die Dateien im Verzeichnis `/usr/lib/vmware-vcops/` nicht global schreibbar sind.
Es dürfen keine Ergebnisse angezeigt werden.
- 7 Führen Sie den Befehl `find /usr/lib/vmware-vcopssuite/ -type f -perm -o=w` aus, um sicherzustellen, dass die Dateien im Verzeichnis `/usr/lib/vmware-vcopssuite/` nicht global schreibbar sind.
Es dürfen keine Ergebnisse angezeigt werden.

PostgreSQL-Client-Authentifizierung konfigurieren

Sie können das System für Client-Authentifizierung konfigurieren. Sie können das System für Local Trust-Authentifizierung konfigurieren. Dadurch kann jeder lokale Benutzer, einschließlich dem Datenbank-Superbenutzer, ohne Eingabe eines Kennworts eine Verbindung als PostgreSQL-Benutzer herstellen. Wenn Sie einen stärkeren Schutz bieten möchten und nicht allen lokalen Benutzerkonten ausreichend vertrauen, verwenden Sie eine andere Authentifizierungsmethode. Die md5-Methode ist standardmäßig festgelegt. Überprüfen Sie, ob md5 für alle lokalen und Host-Verbindungen festgelegt ist.

Die Konfigurationseinstellungen für die Client-Authentifizierung für die Postgres-Serviceinstanz finden Sie in `/storage/db/vcops/vpostgres/data/pg_hba.conf`. Überprüfen Sie, ob md5 für alle lokalen und Host-Verbindungen festgelegt ist.

Sie Konfigurationseinstellungen für die Client-Authentifizierung für die Postgres-Repl-Serviceinstanz finden Sie in `/storage/db/vcops/vpostgres/repl/pg_hba.conf`. Überprüfen Sie, ob md5 für alle lokalen und Host-Verbindungen festgelegt ist.

HINWEIS Ändern Sie die Clientkonfigurationseinstellungen für das Postgres-Benutzerkonto nicht.

Apache-Konfiguration

Durchsuchen des Web Directory deaktivieren

Stellen Sie als Best Practice für die Sicherheit sicher, dass ein Benutzer ein Verzeichnis nicht durchsuchen kann, da dies das Risiko für „Directory-Traversal“-Angriffe erhöht.

Vorgehensweise

- ◆ Überprüfen Sie, ob das Durchsuchen des Web Directory für alle Verzeichnisse deaktiviert ist.
 - a Öffnen Sie die Dateien `/etc/apache2/default-server.conf` und `/usr/lib/vmware-vcopsuite/utilities/conf/vcops-apache.conf` in einem Texteditor.
 - b Überprüfen Sie, dass für jede `<Directory>`-Auflistung die Option namens `Indexes` für das relevante Tag aus der Zeile `Options` ausgeschlossen ist.

Entfernen des Beispielcodes für den Apache2-Server

Apache enthält die folgenden beiden CGI-Beispielskripts (Common Gateway Interface): `printenv` und `test-cgi`. Ein Produktionswebserver darf nur Komponenten enthalten, die für den Betrieb notwendig sind. Es besteht die Möglichkeit, dass diese Komponenten wichtige Informationen über das System für Angreifer offenlegen.

Als Best Practice für die Sicherheit löschen Sie die CGI-Skripts aus dem Verzeichnis `cgi-bin`.

Vorgehensweise

- ◆ Führen Sie zum Entfernen der Skripts `test-cgi` und `prinenv` die folgenden Befehle aus:


```
rm /usr/share/doc/packages/apache2/test-cgi und rm /usr/share/doc/packages/apache2/printenv.
```

Überprüfen von Server-Token für den Apache2-Server

Im Rahmen des Systemhärtungsvorgangs überprüfen Sie Server-Token für den Apache2-Server. Der Webserver-Antwortheader einer HTTP-Antwort kann verschiedene Felder mit Informationen enthalten. Dazu zählen die angeforderte HTML-Seite, Typ und Version des Webservers, Betriebssystem und Version sowie dem Webserver zugeordnete Ports. Auf diese Weise erhalten böswillige Benutzer wichtige Informationen, ohne umfangreiche Werkzeuge einsetzen zu müssen.

Für die Direktive `ServerTokens` muss `Prod` festgelegt werden. Beispielsweise `ServerTokens Prod`. Diese Direktive steuert, ob das Antwortheader-Feld des Servers, das an Clients zurückgesendet wird, eine Beschreibung des Betriebssystems und Informationen über kompilierte Module enthält.

Vorgehensweise

- 1 Führen Sie zur Überprüfung der Server-Token den folgenden Befehl aus: `cat /etc/apache2/sysconfig.d/global.conf | grep ServerTokens`.
- 2 Führen Sie den folgenden Befehl aus, um `ServerTokens OS` in `ServerTokens Prod` zu ändern: `sed -i 's/\(ServerTokens\s\+\)OS/\1Prod/g' /etc/apache2/sysconfig.d/global.conf`.

Deaktivieren der Trace-Methode für den Apache2-Server

In standardmäßigen Produktionsumgebungen können mithilfe von Diagnosefunktionen unerkannte Schwachstellen aufgedeckt werden, die Daten gefährden. Um den Missbrauch von Daten zu verhindern, deaktivieren Sie die HTTP-Methode Trace.

Vorgehensweise

- 1 Führen Sie den folgenden Befehl aus, um die Trace-Methode für den Apache2-Server zu überprüfen:

```
grep TraceEnable /usr/lib/vmware-vcopsuite/utilities/conf/vcops-apache.conf.
```
- 2 Führen Sie den folgenden Befehl aus, um die Trace-Methode für den Apache2-Server zu deaktivieren:

```
sed -i "/^[^#]*TraceEnable/ c\TraceEnable off" /usr/lib/vmware-vcopsuite/utilities/conf/vcops-apache.conf.
```

Konfigurationsmodi deaktivieren

Wenn Sie vRealize Operations Manager installieren, konfigurieren oder warten, können Sie die Konfiguration oder Einstellungen als Best Practice so ändern, dass Fehlerbehebung und Debugging Ihrer Installation ermöglicht werden.

Katalogisieren und prüfen Sie alle vorgenommenen Änderungen, um sicherzustellen, dass sie korrekt abgesichert sind. Veröffentlichen Sie die Änderungen erst, wenn Sie sicher sind, dass Ihre Konfiguration korrekt abgesichert ist.

Verwalten unwichtiger Softwarekomponenten

Um Sicherheitsrisiken zu minimieren, entfernen Sie unwichtige Software von Ihren vRealize Operations Manager-Host-Maschinen oder konfigurieren Sie diese.

Konfigurieren Sie jegliche Software, die Sie nicht entfernen, entsprechend den Empfehlungen des Herstellers und den Best Practices für die Sicherheit, um die Gefahr von Sicherheitsverstößen zu minimieren.

Sichern des USB-Massenspeicher-Handlers

Sichern Sie den USB-Massenspeicher-Handler, um zu verhindern, dass er bei vRealize-Appliances standardmäßig geladen wird, und um zu verhindern, dass er von den vRealize-Appliances als USB-Geräte-Händler verwendet wird. Potenzielle Angreifer können diesen Handler ausnutzen, um Schadsoftware zu installieren.

Vorgehensweise

- 1 Öffnen Sie die Datei `/etc/modprobe.conf.local` in einem Texteditor.
- 2 Stellen Sie sicher, dass die Zeile `install usb-storage /bin/true` in der Datei vorhanden ist.
- 3 Speichern und schließen Sie die Datei.

Sichern des Bluetooth-Protokoll-Handlers

Sichern Sie den Bluetooth-Protokoll-Handler auf Ihren vRealize-Appliances, damit er nicht von potenziellen Angreifern ausgenutzt werden kann.

Das Binden des Bluetooth-Protokolls an den Netzwerk-Stack ist nicht erforderlich und kann die Angriffsfläche des Hosts vergrößern. Verhindern Sie, dass der Bluetooth-Protokoll-Handler standardmäßig auf vRealize-Appliances geladen wird.

Vorgehensweise

- 1 Öffnen Sie die Datei `/etc/modprobe.conf.local` in einem Texteditor.

- 2 Stellen Sie sicher, dass die Zeile `install bluetooth /bin/true` in der Datei vorhanden ist.
- 3 Speichern und schließen Sie die Datei.

Sichern des Stream Control Transmission Protocol

Verhindern Sie, dass das Stream Control Transmission Protocol-Modul (SCTP) standardmäßig auf vRealize-Appliances geladen wird. Potenzielle Angreifer können dieses Protokoll ausnutzen, um Ihr System zu kompromittieren.

Konfigurieren Sie Ihr System so, dass das SCTP-Modul nur dann geladen wird, wenn es absolut notwendig ist. SCTP ist ein nicht verwendetes IETF-standardisiertes Transport Layer-Protokoll. Durch das Binden dieses Protokolls an den Netzwerk-Stack wird die Angriffsfläche des Hosts vergrößert. Nicht berechtigte lokale Prozesse können dazu führen, dass der Kernel einen Protokoll-Handler dynamisch lädt, indem sie mit dem Protokoll ein Socket öffnen.

Vorgehensweise

- 1 Öffnen Sie die Datei `/etc/modprobe.conf.local` in einem Texteditor.
- 2 Stellen Sie sicher, dass die folgende Zeile in der Datei vorhanden ist.


```
install sctp /bin/true
```
- 3 Speichern und schließen Sie die Datei.

Sichern des Datagram Congestion Control Protocol

Verhindern im Rahmen Ihrer Systemabhärtungsaktivitäten, dass das Datagram Congestion Control Protocol-Modul (DCCP) standardmäßig auf vRealize-Appliances geladen wird. Potenzielle Angreifer können dieses Protokoll ausnutzen, um Ihr System zu kompromittieren.

Vermeiden Sie das Laden des DCCP-Moduls, sofern es nicht absolut notwendig ist. DCCP ist ein vorgeschlagenes Transport Layer Protocol, das nicht verwendet wird. Durch das Binden dieses Protokolls an den Netzwerk-Stack wird die Angriffsfläche des Hosts vergrößert. Nicht berechtigte lokale Prozesse können dazu führen, dass der Kernel einen Protokoll-Handler dynamisch lädt, indem sie mit dem Protokoll ein Socket öffnen.

Vorgehensweise

- 1 Öffnen Sie die Datei `/etc/modprobe.conf.local` in einem Texteditor.
- 2 Stellen Sie sicher, dass die DCCP-Zeilen in der Datei vorhanden sind.


```
install dccp /bin/true
install dccp_ipv4 /bin/true
install dccp_ipv6 /bin/true
```
- 3 Speichern und schließen Sie die Datei.

Sichern des Reliable Datagram Sockets-Protokoll

Verhindern im Rahmen Ihrer Systemabhärtungsaktivitäten, dass das Reliable Datagram Sockets-Protokoll (RDS) standardmäßig auf vRealize-Appliances geladen wird. Potenzielle Angreifer können dieses Protokoll ausnutzen, um Ihr System zu kompromittieren.

Durch das Binden des RDS-Protokolls an den Netzwerk-Stack wird die Angriffsfläche des Hosts vergrößert. Nicht berechtigte lokale Prozesse können dazu führen, dass der Kernel einen Protokoll-Handler dynamisch lädt, indem sie mit dem Protokoll ein Socket öffnen.

Vorgehensweise

- 1 Öffnen Sie die Datei `/etc/modprobe.conf.local` in einem Texteditor.

- 2 Stellen Sie sicher, dass die Zeile `install rds /bin/true` in der Datei vorhanden ist.
- 3 Speichern und schließen Sie die Datei.

Transparent Inter-Process Communication-Protokoll sichern

Verhindern sie im Rahmen Ihrer Systemabhärtungsaktivitäten, dass das Transparent Inter-Process Communication-Protokoll (TIPC) standardmäßig auf den Host-Maschinen Ihrer virtuellen Appliance geladen wird. Potenzielle Angreifer können dieses Protokoll ausnutzen, um Ihr System zu kompromittieren.

Durch das Binden des TIPC-Protokolls an den Netzwerk-Stack wird die Angriffsfläche des Hosts vergrößert. Nicht berechnete lokale Prozesse können dazu führen, dass der Kernel einen Protokoll-Handler dynamisch lädt, indem sie mit dem Protokoll ein Socket öffnen.

Vorgehensweise

- 1 Öffnen Sie die Datei `/etc/modprobe.conf.local` in einem Texteditor.
- 2 Stellen Sie sicher, dass die Zeile `install tipc /bin/true` in der Datei vorhanden ist.
- 3 Speichern und schließen Sie die Datei.

Sichern des Internet Packet Exchange-Protokolls

Verbindern Sie, dass das Internetwork Packet Exchange-Protokoll (IPX) standardmäßig auf vRealize-Appliances geladen wird. Potenzielle Angreifer können dieses Protokoll ausnutzen, um Ihr System zu kompromittieren.

Vermeiden Sie das Laden des IPX-Protokolls, sofern es nicht absolut notwendig ist. Das IPX-Protokoll ist ein veraltetes Network Layer-Protokoll. Durch das Binden dieses Protokolls an den Netzwerk-Stack wird die Angriffsfläche des Hosts vergrößert. Nicht berechnete lokale Prozesse können dazu führen, dass das System einen Protokoll-Handler dynamisch lädt, indem sie mit dem Protokoll ein Socket öffnen.

Vorgehensweise

- 1 Öffnen Sie die Datei `/etc/modprobe.conf.local` in einem Texteditor.
- 2 Stellen Sie sicher, dass die Zeile `install ipx /bin/true` in der Datei vorhanden ist.
- 3 Speichern und schließen Sie die Datei.

Sichern des Appletalk-Protokolls

Verhindern Sie, dass das Appletalk-Protokoll standardmäßig auf vRealize-Appliances geladen wird. Potenzielle Angreifer können dieses Protokoll ausnutzen, um Ihr System zu kompromittieren.

Vermeiden Sie das Laden des Appletalk-Protokolls, sofern es nicht absolut notwendig ist. Durch das Binden dieses Protokolls an den Netzwerk-Stack wird die Angriffsfläche des Hosts vergrößert. Nicht berechnete lokale Prozesse können dazu führen, dass das System einen Protokoll-Handler dynamisch lädt, indem sie mit dem Protokoll ein Socket öffnen.

Vorgehensweise

- 1 Öffnen Sie die Datei `/etc/modprobe.conf.local` in einem Texteditor.
- 2 Stellen Sie sicher, dass die Zeile `install appletalk /bin/true` in der Datei vorhanden ist.
- 3 Speichern und schließen Sie die Datei.

Sichern des DECnet-Protokolls

Verhindern Sie, dass das DECnet-Protokoll standardmäßig auf Ihrem System geladen wird. Potenzielle Angreifer können dieses Protokoll ausnutzen, um Ihr System zu kompromittieren.

Vermeiden Sie das Laden des DECnet-Protokolls, sofern es nicht absolut notwendig ist. Durch das Binden dieses Protokolls an den Netzwerk-Stack wird die Angriffsfläche des Hosts vergrößert. Nicht berechtigte lokale Prozesse können dazu führen, dass das System einen Protokoll-Handler dynamisch lädt, indem sie mit dem Protokoll ein Socket öffnen.

Vorgehensweise

- 1 Öffnen Sie die DECnet-Protokolldatei `/etc/modprobe.conf.local` in einem Texteditor.
- 2 Stellen Sie sicher, dass die Zeile `install decnet /bin/true` in der Datei vorhanden ist.
- 3 Speichern und schließen Sie die Datei.

Sichern des Firewire-Moduls

Verhindern Sie, dass das Firewire-Modul standardmäßig auf vRealize-Appliances geladen wird. Potenzielle Angreifer können dieses Protokoll ausnutzen, um Ihr System zu kompromittieren.

Vermeiden Sie das Laden des Firewire-Moduls, sofern es nicht absolut notwendig ist.

Vorgehensweise

- 1 Öffnen Sie die Datei `/etc/modprobe.conf.local` in einem Texteditor.
- 2 Stellen Sie sicher, dass die Zeile `install ieee1394 /bin/true` in der Datei vorhanden ist.
- 3 Speichern und schließen Sie die Datei.

Kernel-Meldungsprotokollierung

Die Spezifikation `kernel.printk` in der Datei `/etc/sysctl.conf` legt die Spezifikationen für die Kernel-Druckprotokollierung fest.

Es sind 4 Werte festgelegt:

- `console loglevel`. Die niedrigste Priorität der Meldungen, die an die Konsole gedruckt werden.
- `default loglevel`. Die niedrigste Stufe für Meldungen ohne spezielle Stufe.
- Die niedrigste mögliche Stufe für die Konsolenprotokollierungsstufe.
- Der Standardwert für die Konsolenprotokollierungsstufe.

Es gibt acht mögliche Einträge pro Wert.

- `define KERN_EMERG "<0>" /* system is unusable */`
- `define KERN_ALERT "<1>" /* action must be taken immediately */`
- `define KERN_CRIT "<2>" /* critical conditions */`
- `define KERN_ERR "<3>" /* error conditions */`
- `define KERN_WARNING "<4>" /* warning conditions */`
- `define KERN_NOTICE "<5>" /* normal but significant condition */`
- `define KERN_INFO "<6>" /* informational */`
- `define KERN_DEBUG "<7>" /* debug-level messages */`

Legen Sie die `kernel.printk`-Werte auf `3 4 1 7` fest und stellen Sie sicher, dass die Zeile `kernel.printk=3 4 1 7` in der Datei `/etc/sysctl.conf` vorhanden ist.

Auf Linux installierte Bereitstellung

Sie können den Network Time Protocol-Dienst (NTP-Dienst) aktivieren und sicherstellen, dass das System mit sicheren Übertragungskanälen bereitgestellt wird.

NTP-Service aktivieren

Für kritisches Zeit-Sourcing können Sie die Host-Zeitsynchronisierung deaktivieren und das Network Time Protocol (NTP) verwenden. NTP in Produktion bedeutet, Benutzeraktionen akkurat zu verfolgen und potenziell schädliche Angriffe und Eindringlinge durch akkurates Auditing und Protokollierung zu erkennen.

Der NTP-Daemon ist auf der Appliance enthalten und wird verwendet, um synchronisierte Zeitserver bereitzustellen. Sie finden die Konfigurationsdatei für NTP in `/etc/ntp.conf`.

TLS für Daten während der Übertragung

Als Best Practice für die Sicherheit müssen Sie sicherstellen, dass das System mit sicheren Übertragungskanälen bereitgestellt wird.

Starke Protokolle für vRealize Operations Manager konfigurieren

Protokolle wie SSLv2 und SSLv3 werden nicht mehr als sicher erachtet. Unterstützen Sie als Best Practice für die Sicherheit nur die TLS-Protokolle.

Vor der Produktion müssen Sie überprüfen, ob SSLv2 und SSLv3 deaktiviert sind.

vRealize Operations Manager für die Verwendung starker Verschlüsselungen konfigurieren

Die Verschlüsselungsstärke, die in einer TLS-Sitzung verwendet wird, wird durch die Verschlüsselung bestimmt, die zwischen dem Server und dem Browser ausgehandelt wird. Um sicherzustellen, dass nur starke Verschlüsselungen ausgewählt werden, müssen Sie den Server dahin gehend ändern, dass die Verwendung schwacher Verschlüsselungen deaktiviert wird. Außerdem müssen die Verschlüsselungen in einer geeigneten Reihenfolge konfiguriert werden. Sie müssen den Server so konfigurieren, dass er nur starke Verschlüsselungen unterstützt und dass ausreichend große Schlüsselgrößen verwendet werden.

Schwache Verschlüsselungen deaktivieren

Deaktivieren Sie Verschlüsselungs-Suites, die keine Authentifizierung ermöglichen, wie z. B. NULL-Verschlüsselungs-Suites, NULL oder eNULL. Wenn keine Authentifizierung stattfindet, sind sie anfällig für Man-in-the-Middle-Angriffe.

Außerdem müssen Sie anonymen Diffie-Hellman-Schlüsselaustausch (ADH), Verschlüsselungen auf Exportebene (EXP, Verschlüsselungen, die DES enthalten), Schlüsselgrößen kleiner als 128 Bits für die Verschlüsselung von Nutzlastdatenverkehr, die Verwendung von MD5 als Hashing-Mechanismus für Nutzlastdatenverkehr, IDEA-Verschlüsselungs-Suites und RC4-Verschlüsselungs-Suites deaktivieren, weil diese anfällig für Angriffe sind.

Schwache Verschlüsselungen in Apache HTTPD-Handler deaktivieren

Deaktivieren Sie schwache Verschlüsselungen und aktivieren Sie starke Verschlüsselungen, die in Apache HTTPD-Handler verwendet werden. Um Man-in-the-Middle-Angriffe zu verhindern, vergleichen Sie die Apache HTTPD-Handler-Verschlüsselungen auf dem vRealize Operations Manager mit der Liste zulässiger Verschlüsselungen und deaktivieren Sie alle Verschlüsselungen, die als schwach erachtet werden.

Vorgehensweise

- 1 Öffnen Sie die Datei `/usr/lib/vmware-vcopsuite/utilities/conf/vcops-apache.conf` in einem Texteditor.
- 2 Überprüfen Sie, ob die Datei die Zeile `SSLCipherSuite HIGH:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:!DH:@STRENGTH` enthält.
- 3 Speichern und schließen Sie die Datei.

Diffie-Hellman-Schlüsselaustausch aktivieren

Diffie-Hellman-Schlüsselaustausch hat einige Schwachstellen. Sie müssen alle Verschlüsselungs-Suites deaktivieren, die DH, DHE und EDH enthalten. Diese Verschlüsselungs-Suites sind standardmäßig deaktiviert. Sie können bei Bedarf aktiviert werden.

Vorgehensweise

- 1 Öffnen Sie die Datei `/usr/lib/vmware-vcopsuite/utilities/conf/vcops-apache.conf`.
- 2 Suchen Sie die Zeile `SSLCipherSuite HIGH:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:!DH:@STRENGTH`.
- 3 Entfernen Sie `!DH:`, sodass die Zeile wie folgt lautet: `SSLCipherSuite HIGH:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:@STRENGTH`.
- 4 Speichern und schließen Sie die Datei.

Konfigurationsmodi deaktivieren

Wenn Sie vRealize Operations Manager installieren, konfigurieren oder warten, können Sie die Konfiguration oder Einstellungen als Best Practice so ändern, dass Fehlerbehebung und Debugging Ihrer Installation ermöglicht werden.

Katalogisieren und prüfen Sie alle vorgenommenen Änderungen, um sicherzustellen, dass sie korrekt abgesichert sind. Veröffentlichen Sie die Änderungen erst, wenn Sie sicher sind, dass Ihre Konfiguration korrekt abgesichert ist.

Überprüfen der sicheren Konfiguration des Hostservers

Für den sicheren Betrieb von vRealize Operations Manager müssen Sie die Abhärtungsaktivitäten sichern und überprüfen.

Weitere Informationen dazu entnehmen Sie der Red Hat Enterprise Linux 6-Abhärtungsanleitung und den Sicherheitsrichtlinien Ihres Unternehmens.

Endpoint Operations Management -Agent

Der Endpoint Operations Management-Agent fügt vRealize Operations Manager agentenbasierte Entdeckungs- und Überwachungsfähigkeiten hinzu.

Der Endpoint Operations Management-Agent wird direkt auf den Hosts installiert und kann sich auf der gleichen Vertrauensebene wie der Endpoint Operations Management-Server befinden. Aus diesem Grund müssen Sie überprüfen, ob die Agenten sicher installiert sind.

Best Practices für die Sicherheit bei Ausführen von Endpoint Operations Management -Agenten

Sie müssen bestimmte Best Practices für die Sicherheit befolgen, wenn Sie Benutzerkonten verwenden.

- Entfernen Sie für eine unbeaufsichtigte Installation alle Zugriffsberechtigungen und Serverzertifikat-Thumbprints, die in der Datei `AGENT_HOME/conf/agent.properties` gespeichert sind.
- Verwenden Sie ein vRealize Operations Manager-Benutzerkonto, das speziell für die Endpoint Operations Management-Agentenregistrierung reserviert ist. Weitere Informationen dazu finden Sie unter dem Thema „Rollen und Berechtigungen“ in vRealize Operations Manager in der vRealize Operations Manager-Hilfe.
- Deaktivieren Sie das vRealize Operations Manager-Benutzerkonto, das Sie für Agentenregistrierung verwenden, nachdem die Installation abgeschlossen ist. Sie müssen den Zugriff des Benutzers für Administrationsaktivitäten am Agenten aktivieren. Weitere Informationen dazu finden Sie unter dem Thema Konfigurieren von Benutzern und Gruppen in vRealize Operations Manager in der vRealize Operations Manager-Hilfe.
- Wenn ein System, auf dem ein Agent ausgeführt wird, kompromittiert wurde, können Sie das Agentenzertifikat widerrufen mithilfe der vRealize Operations Manager-Benutzeroberfläche widerrufen, indem Sie die Agentenressource entfernen. Weitere Informationen dazu finden Sie im Abschnitt „Widerrufen eines Agenten“.

Minimal erforderliche Berechtigungen für Agentenfunktionalität

Sie benötigen Berechtigungen zum Installieren und Ändern eines Service. Wenn Sie einen laufenden Prozess erkennen wollen, muss das Benutzerkonto, das Sie zum Ausführen des Agenten verwenden, auch Berechtigungen für den Zugriff auf die Prozesse und Programme haben. Für Installationen auf dem Windows-Betriebssystem benötigen Sie Berechtigungen zum Installieren und Ändern eines Service. Für Linux-Installationen benötigen Sie die Berechtigung zum Installieren des Agentenservice, wenn Sie den Agenten mit einem RPM-Installationsprogramm installieren.

Die minimalen Anmeldeinformationen, die erforderlich sind, damit sich der Agent am vRealize Operations Manager-Server anmeldet, sind jene, die der Benutzer mit Agentenmanagerrolle hat, ohne Zuweisung zu Objekten innerhalb des Systems.

Linux-basierte Plattformdateien und Berechtigungen

Nachdem Sie den Endpoint Operations Management-Agenten installiert haben, ist der Besitzer der Benutzer, der den Agenten installiert.

Das Installationsverzeichnis und die Dateiberechtigungen wie 600 und 700 sind auf den Besitzer festgelegt, wenn der Benutzer, der den Endpoint Operations Management-Agenten installiert, die TAR-Datei extrahiert oder den RPM installiert.

HINWEIS Wenn Sie die ZIP-Datei extrahieren, werden die Dateiberechtigungen unter Umständen nicht korrekt angewendet. Vergewissern Sie sich, dass die Berechtigungen korrekt sind.

Alle Dateien, die vom Agenten erstellt und geschrieben werden, haben 700-Berechtigungen, wobei der Besitzer der Benutzer ist, der den Agenten ausführt.

Tabelle 3-1. Linux-Dateien und Berechtigungen

Verzeichnis oder Datei	Berechtigungen	Gruppen oder Benutzer	Lesen	Schreiben	Ausführen
<i>agent directory/bin</i>	700	Besitzer	Ja	Ja	Ja
		Gruppe	Nein	Nein	Nein

Tabelle 3-1. Linux-Dateien und Berechtigungen (Fortsetzung)

Verzeichnis oder Datei	Berechtigungen	Gruppen oder Benutzer	Lesen	Schreiben	Ausführen
		Alle	Nein	Nein	Nein
<i>agent directory/conf</i>	700	Besitzer	Ja	Ja	Ja
		Gruppe	Nein	Nein	Nein
		Alle	Nein	Nein	Nein
<i>agent directory/log</i>	700	Besitzer	Ja	Ja	Nein
		Gruppe	Nein	Nein	Nein
		Alle	Nein	Nein	Nein
<i>agent directory/data</i>	700	Besitzer	Ja	Ja	Ja
		Gruppe	Nein	Nein	Nein
		Alle	Nein	Nein	Nein
<i>agent directory/bin/ep-agent.bat</i>	600	Besitzer	Ja	Ja	Nein
		Gruppe	Nein	Nein	Nein
		Alle	Nein	Nein	Nein
<i>agent directory/bin/ep-agent.sh</i>	700	Besitzer	Ja	Ja	Ja
		Gruppe	Nein	Nein	Nein
		Alle	Nein	Nein	Nein
<i>agent directory/conf/*</i> (alle Dateien im Verzeichnis <i>conf</i>)	600	Besitzer	Ja	Ja	Ja
		Gruppe	Nein	Nein	Nein
		Alle	Nein	Nein	Nein
<i>agent directory/log/*</i> (alle Dateien im Verzeichnis <i>log</i>)	600	Besitzer	Ja	Ja	Nein
		Gruppe	Nein	Nein	Nein
		Alle	Nein	Nein	Nein
<i>agent directory/data/*</i> (alle Dateien im Verzeichnis <i>data</i>)	600	Besitzer	Ja	Ja	Nein
		Gruppe	Nein	Nein	Nein
		Alle	Nein	Nein	Nein

Windows-basierte Plattformdateien und Berechtigungen

Für eine Windows-basierte Installation des Endpoint Operations Management-Agenten muss der Benutzer, der den Agenten installiert, Berechtigungen zum Installieren und Ändern des Dienstes haben.

Nachdem Sie den Endpoint Operations Management-Agenten installiert haben, sollte der Installationsordner einschließlich aller Unterverzeichnisse und Dateien nur für das SYSTEM, die Administratorgruppe und den Installationsbenutzer zugänglich sein. Wenn Sie den Endpoint Operations Management-Agenten mit *ep-agent.bat* installieren, stellen Sie sicher, dass der Abhärtungsvorgang erfolgreich ist. Als Benutzer, der den Agenten installiert, empfehlen wir Ihnen, alle Fehlermeldungen zu beachten. Wenn der Abhärtungsvorgang fehlschlägt, kann der Benutzer diese Berechtigungen manuell anwenden.

Tabelle 3-2. Windows-Dateien und Berechtigungen

Verzeichnis oder Datei	Gruppen oder Benutzer	Vollständige Kontrolle	Ändern	Lesen und ausführen	Lesen	Schreiben
<agent directory>/bin	SYSTEM	Ja	-	-	-	-
	Administrator	Ja	-	-	-	-
	Installationsbenutzer	Ja	-	-	-	-
	Benutzer		-	-	-	-
<agent directory>/conf	SYSTEM	Ja	-	-	-	-
	Administrator	Ja	-	-	-	-
	Installationsbenutzer	Ja	-	-	-	-
	Benutzer		-	-	-	-
<agent directory>/log	SYSTEM	Ja	-	-	-	-
	Administrator	Ja	-	-	-	-
	Installationsbenutzer	Ja	-	-	-	-
	Benutzer		-	-	-	-
<agent directory>/data	SYSTEM	Ja	-	-	-	-
	Administrator	Ja	-	-	-	-
	Installationsbenutzer	Ja	-	-	-	-
	Benutzer		-	-	-	-
<agent directory>/bin/hq-agent.bat	SYSTEM	Ja	-	-	-	-
	Administrator	Ja	-	-	-	-
	Installationsbenutzer	Ja	-	-	-	-
	Benutzer		-	-	-	-
<agent directory>/bin/hq-agent.sh	SYSTEM	Ja	-	-	-	-
	Administrator	Ja	-	-	-	-
	Installationsbenutzer	Ja	-	-	-	-
	Benutzer		-	-	-	-
<agent directory>/conf/* (alle Dateien im Verzeichnis conf)	SYSTEM	Ja	-	-	-	-
	Administrator	Ja	-	-	-	-
	Installationsbenutzer	Ja	-	-	-	-
	Benutzer		-	-	-	-
<agent directory>/log/* (alle Dateien im Verzeichnis log)	SYSTEM	Ja	-	-	-	-
	Administrator	Ja	-	-	-	-
	Installationsbenutzer	Ja	-	-	-	-
	Benutzer		-	-	-	-

Tabelle 3-2. Windows-Dateien und Berechtigungen (Fortsetzung)

Verzeichnis oder Datei	Gruppen oder Benutzer	Vollständige Kontrolle	Ändern	Lesen und ausführen	Lesen	Schreiben
<agent directory>/data/* (alle Dateien im Verzeichnis data)	SYSTEM	Ja	-	-	-	-
	Administrator	Ja	-	-	-	-
	Installationsbenutzer	Ja	-	-	-	-
	Benutzer		-	-	-	-

Ports auf Agenten-Host öffnen

Der Agentenprozess überwacht Befehle auf zwei Ports, 127.0.0.1:2144 und 127.0.0.1:32000, die konfiguriert werden können. Diese Ports können zufällig zugewiesen werden, sodass die exakte Portnummer abweichen kann. Der Agent öffnen keine Ports auf externen Schnittstellen.

Tabelle 3-3. Minimal erforderliche Ports

Port	Protokoll	Richtung	Anmerkungen
443	TCP	Ausgang	Vom Agenten für ausgehende Verbindungen über HTTP, TCP oder ICMP verwendet.
2144	TCP	Listening	Nur intern. Konfigurierbar. Für Inter-Process-Kommunikation zwischen dem Agenten und der Befehlszeile verwendet, die ihn lädt und konfiguriert. Der Agentenprozess überwacht diesen Port. HINWEIS Die Portnummer wird zufällig zugewiesen und kann abweichen.
32000	TCP	Listening	Nur intern. Konfigurierbar. Für Inter-Process-Kommunikation zwischen dem Agenten und der Befehlszeile verwendet, die ihn lädt und konfiguriert. Der Agentenprozess überwacht diesen Port. HINWEIS Die Portnummer wird zufällig zugewiesen und kann abweichen.

Widerrufen eines Agenten

Wenn Sie einen Agenten aus irgendeinem Grund widerrufen müssen, wenn beispielsweise ein System mit einem laufenden Agenten kompromittiert wurde, können Sie die Agentenressource aus dem System löschen. Alle nachfolgenden Anfragen bestehen die Verifizierung nicht.

Verwenden Sie die vRealize Operations Manager-Benutzeroberfläche, um das Agentenzertifikat zu widerrufen, indem Sie die Agentenressource entfernen. Weitere Informationen finden Sie unter „[Entfernen der Agentenressource](#)“, auf Seite 39.

Wenn das System wieder sicher ist, können Sie den Agenten wieder einsetzen. Weitere Informationen finden Sie unter „[Agentenressource wieder einsetzen](#)“, auf Seite 40.

Entfernen der Agentenressource

Sie können vRealize Operations Manager verwenden, um das Agentenzertifikat zu widerrufen, indem Sie die Agentenressource entfernen.

Voraussetzungen

Um die Kontinuität der Ressource mit den zuvor aufgezeichneten Metrikdaten aufrecht zu erhalten, notieren Sie den Endpoint Operations Management-Agenten-Token, der in den Ressourcendetails angezeigt wird.

Vorgehensweise

- 1 Navigieren Sie zum Bestands-Explorer auf der vRealize Operations Manager-Benutzeroberfläche.
- 2 Öffnen Sie den Strukturbaum der Adaptertypen.
- 3 Öffnen Sie die EP Ops-Adapterliste.
- 4 Wählen Sie **EP Ops Agent - *HOST_DNS_NAME*** aus.
- 5 Klicken Sie auf **Objekt bearbeiten**.
- 6 Notieren Sie die Agenten-ID, die der Agenten-Token-Zeichenfolge entspricht.
- 7 Schließen Sie das Dialogfeld „Objekt bearbeiten“.
- 8 Wählen Sie **EP Ops Agent - *HOST_DNS_NAME*** aus und klicken Sie auf **Objekt löschen**.

Agentenressource wieder einsetzen

Wenn der sichere Status eines System wiederhergestellt wurde, können Sie einen widerrufenen Agenten wieder einsetzen. Dadurch wird sichergestellt, dass der Agent weiterhin auf denselben Ressourcen berichtet, ohne das historische Daten verloren gehen. Dafür müssen Sie eine neue Token-Datei Endpoint Operations Management mithilfe desselben Tokens erstellen, der vor dem Entfernen der Agentenressource aufgezeichnet wurde. Weitere Informationen dazu finden Sie im Abschnitt „Entfernen der Agentenressource“.

Voraussetzungen

- Halten Sie die notierte Endpoint Operations Management-Token-Zeichenfolge bereit.
- Verwenden Sie den Ressourcen-Token, den Sie vor dem Entfernen der Agentenressource vom vRealize Operations Manager-Server notiert haben.
- Stellen Sie sicher, dass Sie über die Berechtigung „Agent verwalten“ verfügen.

Vorgehensweise

- 1 Erstellen Sie eine Agenten-Token-Datei mit dem Benutzer, den den Agenten ausführt.

Führen Sie zum Beispiel den Befehl aus, um eine Token-Datei zu erstellen, die den Token 123-456-789 enthält.

- Unter Linux:

```
echo 123-456-789 > /etc/epops/epops-token
```

- Unter Windows:

```
echo 123-456-789 > %PROGRAMDATA%\VMware\Ep Ops Agent\epops-token
```

In dem Beispiel wird die Token-Datei auf den standardmäßigen Token-Speicherort für diese Plattform geschrieben.

- 2 Installieren Sie einen neuen Agenten und registrieren Sie ihn auf dem vRealize Operations Manager-Server. Stellen Sie sicher, dass der Agent den Token lädt, den Sie in die Token-Datei eingefügt haben. Sie müssen über die Berechtigung „Agent verwalten“ verfügen, um diese Aktion ausführen zu können.

Rückruf des Agentenzertifikats und Aktualisieren von Zertifikaten

Die Wiederausgabe wird von dem Agenten mithilfe des Befehlszeilenarguments `setup` initiiert. Wenn ein Agent, der bereits registriert ist, das `setup`-Befehlszeilenargument `ep-agent.sh setup` verwendet und die erforderlichen Anmeldeinformationen einträgt, wird ein neuer `registerAgent`-Befehl an den Server gesendet.

Der Server erkennt, dass der Agent bereits registriert ist und sendet dem Agenten ein neues Client-Zertifikat, ohne eine andere Agentenressource zu erstellen. Auf der Agentenseite ersetzt das neue Client-Zertifikat das alte. Wenn das Serverzertifikat geändert wird und Sie den Befehl `ep-agent.sh setup` ausführen, wird eine Meldung angezeigt, die Sie auffordert, dem neuen Zertifikat zu vertrauen. Sie können alternativ den neuen Serverzertifikat-Thumbprint in der Datei `agent.properties` bereitstellen, bevor Sie den Befehl `ep-agent.sh setup` ausführen, damit dieser Vorgang unbeaufsichtigt durchgeführt werden kann.

Voraussetzungen

Verwalten Sie Agentenberechtigungen, um Zertifikate zurück zu rufen oder zu aktualisieren.

Vorgehensweise

- ◆ Führen Sie den Befehl `ep-agent.sh setup` bei Linux-basierten Betriebssystemen auf dem Agenten-Host aus. Führen Sie auf Windows-basierten Betriebssystemen den Befehl `ep-agent.bat setup` aus.

Wenn der Agent erkennt, dass das Serverzertifikat geändert wurde, wird eine Meldung angezeigt. Akzeptieren Sie das Zertifikat, wenn Sie ihm vertrauen und es gültig ist.

Patches und Aktualisieren des Endpoint Operations Management -Agenten

Bei Bedarf stehen neue Endpoint Operations Management-Agentenpakete unabhängig von vRealize Operations Manager-Versionen zur Verfügung.

Patches oder Updates werden für den Endpoint Operations Management-Agenten nicht bereitgestellt. Sie müssen die jeweils aktuelle Version des Agenten mit den letzten Sicherheitskorrekturen installieren. Kritische Sicherheitskorrekturen werden wie in den Anleitungen zu Sicherheitshinweisen von VMware angegeben kommuniziert. Lesen Sie das Thema zu Sicherheitshinweisen.

Zusätzliche Aktivitäten für eine sichere Konfiguration

Überprüfen Sie die Benutzerkonten des Servers, und löschen Sie nicht benötigte Anwendungen von den Hostservern. Blockieren Sie nicht benötigte Ports, und deaktivieren Sie die Dienste, die auf Ihrem Hostserver ausgeführt und nicht benötigt werden.

Benutzerkontoeinstellungen des Servers überprüfen

Wir empfehlen, dass Sie überprüfen, ob unnötige Benutzerkonten für lokale und Domänen-Benutzerkonten und -Einstellungen vorhanden sind.

Beschränken Sie alle Benutzerkonten, die nicht im Zusammenhang mit der Funktionsweise der Applikation stehen, auf jede, die für Verwaltung, Wartung und Fehlerbehebung erforderlich sind. Beschränken Sie den Remote-Zugriff von Domänen-Benutzerkonten auf das Minimum, das für den Betrieb des Servers erforderlich ist. Diese Konten müssen streng kontrolliert und geprüft werden.

Unnötige Anwendungen löschen und deaktivieren

Löschen Sie nicht benötigte Anwendungen von den Host-Servern. Jede zusätzliche und nicht benötigte Anwendung erhöht das Sicherheitsrisiko, da sie unbekannte oder unbehobene Schwachstellen haben kann.

Unnötige Ports und Dienste deaktivieren

Überprüfen Sie die Firewall des Host-Servers hinsichtlich der Liste offener Ports, die Datenverkehr erlauben.

Blockieren Sie alle Ports, die im Abschnitt „[Ports und Protokolle konfigurieren](#)“, auf Seite 52 nicht als Mindestanforderung für vRealize Operations Manager aufgeführt sind oder die nicht erforderlich sind. Prüfen Sie zusätzlich die Dienste, die auf Ihrem Host-Server ausgeführt werden, und deaktivieren Sie all jene, die nicht erforderlich sind.

Netzwerksicherheit und sichere Kommunikation

4

Als Best Practice für die Sicherheit müssen Sie die Einstellungen für die Netzwerksicherheit Ihrer virtuellen VMware Appliances und Host-Maschinen überprüfen und bearbeiten. Außerdem müssen Sie die minimal erforderlichen eingehenden und ausgehenden Ports für vRealize Operations Manager konfigurieren.

Dieses Kapitel behandelt die folgenden Themen:

- „Netzwerkeinstellungen für Virtual Application Installation konfigurieren“, auf Seite 43
- „Ports und Protokolle konfigurieren“, auf Seite 52

Netzwerkeinstellungen für Virtual Application Installation konfigurieren

Um sicherzustellen, dass Ihre VMware Virtual Appliance und Host-Computern nur sichere und wichtige Kommunikation zulassen, überprüfen und bearbeiten Sie die Einstellungen für Netzwerkkommunikation.

Benutzerkontrolle der Netzwerkschnittstellen verhindern

Als Best Practice für die Sicherheit müssen Sie die Möglichkeit der Änderung der Netzwerkschnittstelle auf berechnete Benutzer einschränken. Wenn Benutzer Netzwerkschnittstellen manipulieren, kann das zur Umgehung von Sicherheitsmechanismen für das Netzwerk oder zu Denial-of-Service führen. Stellen Sie sicher, dass die Netzwerkschnittstellen nicht für Benutzerkontrolle konfiguriert sind.

Vorgehensweise

- 1 Um die Benutzereinstellungen zu überprüfen, führen Sie den Befehl `#grep -i '^USERCONT-ROL=' /etc/sysconfig/network/ifcfg*` aus.
- 2 Stellen Sie sicher, dass jede Schnittstelle auf NEIN festgelegt ist.

Warteschlangengröße für TCP-Backlog festlegen

Als Best Practice für die Sicherheit müssen Sie eine standardmäßige Warteschlangengröße für das TCP-Backlog auf VMware-Appliance-Host-Maschinen konfigurieren. Um TCP-Denial- oder Service-Angriffe zu verhindern, legen Sie eine angemessene Standardgröße für die Warteschlange des TCP-Backlogs fest. Die empfohlene Standardeinstellung ist 1280.

Vorgehensweise

- 1 Führen Sie den Befehl `# cat /proc/sys/net/ipv4/tcp_max_syn_backlog` auf jeder VMware-Appliance-Host-Maschine aus.

- 2 Legen Sie die Warteschlangengröße für das TCP-Backlog fest.
 - a Öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
 - b Legen Sie die standardmäßige Warteschlangengröße für das TCP-Backlog durch Hinzufügen des folgenden Eintrags in die Datei fest.

```
net.ipv4.tcp_max_syn_backlog=1280
```

- c Speichern Sie die Änderungen, und schließen Sie die Datei.

ICMPv4 Echos für Broadcast-Adressen ablehnen

Antworten auf das Senden von Internet Control Message Protocol-Echos (ICMP-Echos) bieten einen Angriffspunkt für Verstärkungsangriffe und können das Netzwerk-Mapping durch böartige Agenten ermöglichen. Wenn Sie Ihr System so konfigurieren, dass ICMPv4-Echos ignoriert werden, schützen Sie es vor solchen Angriffen.

Vorgehensweise

- 1 Führen Sie den Befehl `# cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts` aus, um sicherzustellen, dass das System keine Antworten auf ICMP-Echos für Broadcast-Adressen sendet.
- 2 Konfigurieren Sie das Host-System so, dass ICMPv4 Echos für Broadcast-Adressen abgelehnt werden.
 - a Öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
 - b Wenn der Wert für diesen Eintrag nicht auf 1 festgelegt ist, fügen Sie den Eintrag `net.ipv4.icmp_echo_ignore_broadcasts=1` hinzu.
 - c Speichern Sie die Änderungen, und schließen Sie die Datei.

Host-System so konfigurieren, dass IPv4 Proxy ARP deaktiviert wird

Mit IPv4 Proxy ARP kann ein System Antworten auf ARP-Anfragen an einer Schnittstelle im Namen von Hosts senden, die mit einer anderen Schnittstelle verbunden sind. Sie müssen IPv4 Proxy ARP deaktivieren, um den nicht autorisierten Austausch von Informationen zu verhindern. Deaktivieren Sie die Einstellung, um die Weitergabe von Adressinformationen zwischen den angehängten Netzwerksegmenten zu verhindern.

Vorgehensweise

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv4/conf/*/proxy_arp | grep "default|all"` aus, um zu überprüfen, ob Proxy ARP deaktiviert ist.
- 2 Konfigurieren Sie das Host-System so, dass IPv4 Proxy ARP deaktiviert wird.
 - a Öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
 - b Wenn die Werte nicht auf 0 festgelegt sind, fügen Sie die Einträge hinzu, oder aktualisieren Sie die vorhandenen Einträge entsprechend. Legen Sie den Wert auf 0 fest.


```
net.ipv4.conf.all.proxy_arp=0
net.ipv4.conf.default.proxy_arp=0
```
 - c Speichern Sie alle vorgenommenen Änderungen, und schließen Sie die Datei.

Host-System so konfigurieren, dass es IPv4 ICMP Redirect-Meldungen ignoriert

Prüfen Sie als Best Practice für die Sicherheit, ob das Host-System IPv4 Internet Control Message Protocol (ICMP) Redirect-Meldungen ignoriert. Durch eine schadhafte ICMP Redirect-Meldung kann ein Man-in-the-Middle-Angriff durchgeführt werden. Router verwenden ICMP Redirect-Meldungen, um Hosts zu benachrichtigen, dass für ein Ziel eine direktere Weiterleitung vorhanden ist. Diese Meldungen passen die Weiterleitungstabelle des Hosts an und sind nicht authentifiziert.

Vorgehensweise

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv4/conf/*/accept_redirects | egrep "default|all"` auf dem Host-System aus, um zu prüfen, ob das Host-System IPv4 Redirect-Meldungen ignoriert.
- 2 Konfigurieren Sie das Host-System so, dass es IPv4 ICMP Redirect-Meldungen ignoriert.
 - a Öffnen Sie die Datei `/etc/sysctl.conf`.
 - b Wenn die Werte nicht auf `0` festgelegt sind, fügen Sie die folgenden Einträge zur Datei hinzu, oder aktualisieren Sie die vorhandenen Einträge entsprechend. Legen Sie den Wert auf `0` fest.


```
net.ipv4.conf.all.accept_redirects=0
net.ipv4.conf.default.accept_redirects=0
```
 - c Speichern Sie die Änderungen, und schließen Sie die Datei.

Host-System so konfigurieren, dass es IPv6 ICMP Redirect-Meldungen ignoriert

Prüfen Sie als Best Practice für die Sicherheit, ob das Host-System IPv6 Internet Control Message Protocol (ICMP) Redirect-Meldungen ignoriert. Durch eine schadhafte ICMP Redirect-Meldung kann ein Man-in-the-Middle-Angriff durchgeführt werden. Router verwenden ICMP Redirect-Meldungen, um Hosts mitzuteilen, dass für ein Ziel eine direktere Weiterleitung vorhanden ist. Diese Meldungen passen die Weiterleitungstabelle des Hosts an und sind nicht authentifiziert.

Vorgehensweise

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv6/conf/*/accept_redirects | egrep "default|all"` auf dem Host-System aus und prüfen Sie, ob es IPv6 Redirect-Meldungen ignoriert.
- 2 Konfigurieren Sie das Host-System so, dass es IPv6 ICMP Redirect-Meldungen ignoriert.
 - a Öffnen Sie die Datei `/etc/sysctl.conf`, um das Host-System so zu konfigurieren, dass es die IPv6 Redirect-Meldungen ignoriert.
 - b Wenn die Werte nicht auf `0` festgelegt sind, fügen Sie die folgenden Einträge zur Datei hinzu, oder aktualisieren Sie die vorhandenen Einträge entsprechend. Legen Sie den Wert auf `0` fest.


```
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```
 - c Speichern Sie die Änderungen, und schließen Sie die Datei.

Host-System so konfigurieren, dass IPv4 ICMP-Umleitungen abgelehnt werden

Prüfen Sie als Best Practice für die Sicherheit, ob das Host-System IPv4 Internet Control Message Protocol-Umleitungen (ICMP-Umleitungen) ablehnt. Router verwenden ICMP Redirect-Meldungen, um Server darüber zu informieren, dass für ein bestimmtes Ziel eine direkte Weiterleitung vorhanden ist. Diese Meldungen enthalten Informationen aus der Weiterleitungstabelle des Systems, die Teile der Netzwerktopologie offenlegen können.

Vorgehensweise

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv4/conf/*/send_redirects | grep "default|all"` auf dem Host-System aus, um zu prüfen, ob es IPv4 ICMP-Umleitungen ablehnt.
- 2 Konfigurieren Sie das Host-System so, dass IPv4 ICMP-Umleitungen abgelehnt werden.
 - a Öffnen Sie die Datei `/etc/sysctl.conf`, um das Host-System zu konfigurieren.
 - b Wenn die Werte nicht auf `0` festgelegt sind, fügen Sie die folgenden Einträge zur Datei hinzu, oder aktualisieren Sie die vorhandenen Einträge entsprechend. Legen Sie den Wert auf `0` fest.


```
net.ipv4.conf.all.send_redirects=0
net.ipv4.conf.default.send_redirects=0
```
 - c Speichern Sie die Änderungen, und schließen Sie die Datei.

Host-System so konfigurieren, dass IPv4 Martian-Pakete protokolliert werden

Prüfen Sie als Best Practice für die Sicherheit, dass das Host-System IPv4-Martian-Pakete protokolliert. Martian-Pakete enthalten Adressen, von denen das System weiß, dass sie ungültig sind. Konfigurieren Sie das Host-System so dass die Meldungen protokolliert werden, damit Sie falsche Konfigurationen oder Angriffe identifizieren können.

Vorgehensweise

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv4/conf/*/log_martians | grep "default|all"` aus, um zu überprüfen, ob der Host IPv4-Martian-Pakete protokolliert.
- 2 Konfigurieren Sie das Host-System so, dass IPv4 Martian-Pakete protokolliert werden.
 - a Öffnen Sie die Datei `/etc/sysctl.conf`, um das Host-System zu konfigurieren.
 - b Wenn die Werte nicht auf `1` festgelegt sind, fügen Sie die folgenden Einträge zur Datei hinzu, oder aktualisieren Sie die vorhandenen Einträge entsprechend. Legen Sie den Wert auf `1` fest.


```
net.ipv4.conf.all.log_martians=1
net.ipv4.conf.default.log_martians=1
```
 - c Speichern Sie die Änderungen, und schließen Sie die Datei.

Host-System für die Verwendung von IPv4 Reverse Path-Filterung konfigurieren

Konfigurieren Sie Ihre Host-Computer als Best Practice für die Sicherheit so, dass IPv4 Reverse Path-Filterung verwendet wird. Reverse Path-Filterung schützt vor gefälschten Quellenadressen, indem das System veranlasst wird, Pakete mit Quellenadressen zu verwerfen, die keine Weiterleitung haben oder deren Weiterleitung nicht auf die ursprüngliche Schnittstelle verweist.

Konfigurieren Sie Ihr System so, dass Reverse Path-Filterung wann immer möglich verwendet wird. Je nach Systemrolle kann Reverse Path-Filterung dazu führen, dass legitimer Datenverkehr verworfen wird. In diesen Fällen müssen Sie unter Umständen einen weniger strengen Modus verwenden oder die Reverse Path-Filterung vollständig deaktivieren.

Vorgehensweise

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv4/conf/*/rp_filter|grep "default|all"` auf dem Host-System aus, um zu überprüfen, ob das System IPv4 Reverse Path-Filterung verwendet.
- 2 Konfigurieren Sie das Host-System für die Verwendung von IPv4 Reverse Path-Filterung.
 - a Öffnen Sie die Datei `/etc/sysctl.conf`, um das Host-System zu konfigurieren.
 - b Wenn die Werte nicht auf 1 festgelegt sind, fügen Sie die folgenden Einträge zur Datei hinzu, oder aktualisieren Sie die vorhandenen Einträge entsprechend. Legen Sie den Wert auf 1 fest.


```
net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.default.rp_filter=1
```
 - c Speichern Sie die Änderungen, und schließen Sie die Datei.

Host-System so konfigurieren, dass IPv4-Weiterleitung abgelehnt wird

Prüfen Sie als Best Practice für die Sicherheit, dass das Host-System IPv4-Weiterleitungen ablehnt. Wenn IP-Weiterleitung im System konfiguriert ist und es sich nicht um einen designierten Router handelt, kann diese verwendet werden, um die Netzwerksicherheit zu umgehen, indem ein Kommunikationspfad bereitgestellt wird, der nicht von Netzwerkgeräten gefiltert wird.

Vorgehensweise

- 1 Führen Sie den Befehl `# cat /proc/sys/net/ipv4/ip_forward` aus, um zu überprüfen, ob der Host IPv4-Weiterleitung ablehnt.
- 2 Konfigurieren Sie das Host-System so, dass IPv4-Weiterleitung abgelehnt wird.
 - a Öffnen Sie die Datei `/etc/sysctl.conf`, um das Host-System zu konfigurieren.
 - b Wenn der Wert nicht auf 0 festgelegt ist, fügen Sie den folgenden Eintrag zur Datei hinzu, oder aktualisieren Sie den vorhandenen Eintrag entsprechend. Legen Sie den Wert auf 0 fest.


```
net.ipv4.ip_forward=0
```
 - c Speichern Sie die Änderungen, und schließen Sie die Datei.

Das Host-System so konfigurieren, dass die Weiterleitung von IPv4 Source Routed-Paketen abgelehnt wird

Source Routed-Pakete erlauben es der Quelle des Pakets vorzuschlagen, dass Router das Paket auf einem anderen Pfad weiterleiten, als dem im Router konfigurierten, was zur Umgehung der Netzwerksicherheit genutzt werden kann.

Diese Anforderung gilt nur für die Weiterleitung des Source Routed-Datenverkehrs, z. B. wenn IPv4-Weiterleitung aktiviert ist und das System als Router fungiert.

Vorgehensweise

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv4/conf/*/accept_source_route|grep "default|all"` aus, um zu überprüfen, ob das System IPv4 Source Routed-Pakete verwendet.
- 2 Konfigurieren Sie das Host-System so, dass die Weiterleitung von IPv4 Source Routed-Paketen abgelehnt wird.
 - a Öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
 - b Wenn die Werte nicht auf 0 festgelegt sind, stellen Sie sicher, dass `net.ipv4.conf.all.accept_source_route=0` und `net.ipv4.conf.default.accept_source_route=0` auf 0 festgelegt sind.
 - c Speichern und schließen Sie die Datei.

Host-System so konfigurieren, dass IPv6-Weiterleitung abgelehnt wird

Prüfen Sie als Best Practice für die Sicherheit, dass das Host-System IPv6-Weiterleitungen ablehnt. Wenn IPv6-Weiterleitung im System konfiguriert ist und es sich nicht um einen designierten Router handelt, kann diese verwendet werden, um die Netzwerksicherheit zu umgehen, indem ein Kommunikationspfad bereitgestellt wird, der nicht von Netzwerkgeräten gefiltert wird.

Vorgehensweise

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv6/conf/*/forwarding | grep "default|all"` aus, um zu überprüfen, ob der Host IPv6-Weiterleitung ablehnt.
- 2 Konfigurieren Sie das Host-System so, dass IPv6-Weiterleitung abgelehnt wird.
 - a Öffnen Sie die Datei `/etc/sysctl.conf`, um das Host-System zu konfigurieren.
 - b Wenn die Werte nicht auf `0` festgelegt sind, fügen Sie die folgenden Einträge zur Datei hinzu, oder aktualisieren Sie die vorhandenen Einträge entsprechend. Legen Sie den Wert auf `0` fest.


```
net.ipv6.conf.all.forwarding=0
net.ipv6.conf.default.forwarding=0
```
 - c Speichern Sie die Änderungen, und schließen Sie die Datei.

Host-System so konfigurieren, dass IPv4 TCP Syncookies verwendet werden

Als Best Practice für die Sicherheit müssen Sie überprüfen, ob das Host-System IPv4 Transmission Control Protocol (TCP) Syncookies verwendet. Ein TCP SYN-Angriff kann zu einem Denial-of-Service führen, indem die TCP-Verbindungstabelle eines Systems mit Verbindungen im `SYN_RCVD`-Status gefüllt wird. Syncookies werden verwendet, damit eine Verbindung erst dann verfolgt wird, wenn eine ACK empfangen wurde, um zu bestätigen, dass der Initiator eine gültige Verbindung und keine Angriffsquelle aufbauen will.

Diese Technik entspricht nicht vollständig den Standards, wird jedoch nur aktiviert, wenn eine Angriffsbedingung erkannt wird, und sie ermöglicht die Verteidigung des Systems bei gleichzeitiger Bedienung gültiger Anfragen.

Vorgehensweise

- 1 Führen Sie den Befehl `# cat /proc/sys/net/ipv4/tcp_syncookies` aus, um zu überprüfen, ob das Host-System IPv4 TCP Syncookies verwendet.
- 2 Konfigurieren Sie das Host-System so, dass IPv4 TCP Syncookies verwendet werden.
 - a Öffnen Sie die Datei `/etc/sysctl.conf`, um das Host-System zu konfigurieren.
 - b Wenn der Wert nicht auf `1` festgelegt ist, fügen Sie den folgenden Eintrag zur Datei hinzu, oder aktualisieren Sie den vorhandenen Eintrag entsprechend. Legen Sie den Wert auf `1` fest.


```
net.ipv4.tcp_syncookies=1
```
 - c Speichern Sie die Änderungen, und schließen Sie die Datei.

Host-System so konfigurieren, dass IPv6 Router-Advertisements abgelehnt werden

Prüfen Sie als Best Practice für die Sicherheit, ob das Host-System die Annahme von Router-Advertisements und Internet Control Message Protocol-Umleitungen (ICMP-Umleitungen) ablehnt, sofern diese nicht erforderlich sind. Eine Funktion von IPv6 ist, wie Systeme ihre Netzwerkgeräte durch automatische Verwendung von Informationen aus dem Netzwerk konfigurieren können. Aus Sicherheitsgründen sollten wichtige Konfigurationsinformationen vorzugsweise manuell festgelegt werden, anstatt sie nicht authentifiziert aus dem Netzwerk anzunehmen.

Vorgehensweise

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra|grep "default|all"` auf dem Host-System aus, um zu prüfen, ob das System Router-Advertisements und ICMP-Umleitungen ablehnt, sofern diese nicht erforderlich sind.
- 2 Konfigurieren Sie das Host-System so, dass IPv6 Router-Advertisements abgelehnt werden.
 - a Öffnen Sie die Datei `/etc/sysctl.conf`.
 - b Wenn die Werte nicht auf 0 festgelegt sind, fügen Sie die folgenden Einträge zur Datei hinzu, oder aktualisieren Sie die vorhandenen Einträge entsprechend. Legen Sie den Wert auf 0 fest.


```
net.ipv6.conf.all.accept_ra=0
net.ipv6.conf.default.accept_ra=0
```
 - c Speichern Sie die Änderungen, und schließen Sie die Datei.

Host-System so konfigurieren, dass IPv6 Router-Anfragen abgelehnt werden

Prüfen Sie als Best Practice für die Sicherheit, dass das Host-System IPv6 Router-Anfragen ablehnt, sofern diese nicht erforderlich sind. Die Einstellung für Router-Anfragen bestimmt, wie viele Router-Anfragen beim Starten der Schnittstelle gesendet werden. Wenn Adressen statisch zugewiesen werden, müssen keine Anfragen gesendet werden.

Vorgehensweise

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv6/conf/*/router_solicitations|grep "default|all"` aus, um zu überprüfen, ob das Host-System IPv6 Router-Anfragen ablehnt, sofern diese nicht erforderlich sind.
- 2 Konfigurieren Sie das Host-System so, dass IPv6 Router-Anfragen abgelehnt werden.
 - a Öffnen Sie die Datei `/etc/sysctl.conf`.
 - b Wenn die Werte nicht auf 0 festgelegt sind, fügen Sie die folgenden Einträge zur Datei hinzu, oder aktualisieren Sie die vorhandenen Einträge entsprechend. Legen Sie den Wert auf 0 fest.


```
net.ipv6.conf.all.router_solicitations=0
net.ipv6.conf.default.router_solicitations=0
```
 - c Speichern Sie die Änderungen, und schließen Sie die Datei.

Host-System so konfigurieren, dass IPv6 Router-Einstellungen bei Router-Anfragen abgelehnt werden

Prüfen Sie als Best Practice für die Sicherheit, dass Ihr Host-System IPv6 Router-Anfragen ablehnt, sofern diese nicht erforderlich sind. Die Router-Einstellungen werden in der Anfrageneinstellung festgelegt. Wenn Adressen statisch zugewiesen werden, müssen keine Router-Einstellungen für Anfragen empfangen werden.

Vorgehensweise

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_rtr_pref | egrep "default|all"` auf dem Host-System aus, um zu prüfen, ob das Host-System IPv6 Router-Anfragen ablehnt.
- 2 Konfigurieren Sie das Host-System so, dass IPv6 Router-Einstellungen bei Router-Anfragen abgelehnt werden.
 - a Öffnen Sie die Datei `/etc/sysctl.conf`.
 - b Wenn die Werte nicht auf `0` festgelegt sind, fügen Sie die folgenden Einträge zur Datei hinzu, oder aktualisieren Sie die vorhandenen Einträge entsprechend. Legen Sie den Wert auf `0` fest.


```
net.ipv6.conf.all.accept_ra_rtr_pref=0
net.ipv6.conf.default.accept_ra_rtr_pref=0
```
 - c Speichern Sie die Änderungen, und schließen Sie die Datei.

Host-System so konfigurieren, dass IPv6 Router-Präfixe abgelehnt werden

Prüfen Sie als Best Practice für die Sicherheit, dass das Host-System IPv6 Router-Präfixinformationen ablehnt, sofern diese nicht erforderlich sind. Die Einstellung `accept_ra_pinfo` steuert, ob das System Präfixeinstellungen vom Router akzeptiert. Wenn Adressen statisch zugewiesen werden, empfängt das System keine Router-Präfixinformationen.

Vorgehensweise

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_pinfo | egrep "default|all"` aus, um zu überprüfen, ob das System IPv6 Router-Präfixinformationen ablehnt.
- 2 Konfigurieren Sie das Host-System so, dass IPv6 Router-Präfixe abgelehnt werden.
 - a Öffnen Sie die Datei `/etc/sysctl.conf`.
 - b Wenn die Werte nicht auf `0` festgelegt sind, fügen Sie die folgenden Einträge zur Datei hinzu, oder aktualisieren Sie die vorhandenen Einträge entsprechend. Legen Sie den Wert auf `0` fest.


```
net.ipv6.conf.all.accept_ra_pinfo=0
net.ipv6.conf.default.accept_ra_pinfo=0
```
 - c Speichern Sie die Änderungen, und schließen Sie die Datei.

Host-System so konfigurieren, dass Hop-Limit-Einstellungen der IPv6 Router-Advertisements abgelehnt werden

Überprüfen Sie als Best Practice für die Sicherheit, dass das Host-System Hop-Limit-Einstellungen der IPv6 Router-Advertisements ablehnt, sofern diese nicht erforderlich sind. Die Einstellung `accept_ra_defrtr` steuert, ob das System Hop Limit-Einstellungen von einem Router-Advertisement akzeptiert. Durch die Einstellung auf 0 wird verhindert, dass ein Router das standardmäßige IPv6 Hop-Limit für ausgehende Pakete ändert.

Vorgehensweise

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_defrtr | egrep "default|all"` aus, um zu überprüfen, ob das Host-System Hop-Limit-Einstellungen der IPv6 Router-Advertisements ablehnt.
- 2 Wenn diese Werte nicht auf 0 festgelegt sind, konfigurieren Sie das Host-System so, dass Hop-Limit-Einstellungen der IPv6 Router-Advertisements abgelehnt werden.
 - a Öffnen Sie die Datei `/etc/sysctl.conf`.
 - b Wenn die Werte nicht auf 0 festgelegt sind, fügen Sie die folgenden Einträge zur Datei hinzu, oder aktualisieren Sie die vorhandenen Einträge entsprechend. Legen Sie den Wert auf 0 fest.


```
net.ipv6.conf.all.accept_ra_defrtr=0
net.ipv6.conf.default.accept_ra_defrtr=0
```
 - c Speichern Sie die Änderungen, und schließen Sie die Datei.

Host-System so konfigurieren, dass autoconf-Einstellungen der IPv6 Router-Advertisements abgelehnt werden

Prüfen Sie als Best Practice für die Sicherheit, dass das Host-System autoconf-Einstellungen für IPv6 Router-Advertisements ablehnt. Die Einstellung `autoconf` steuert, ob Router-Advertisements dazu führen können, dass das System einer Schnittstelle eine globale Unicast-Adresse zuweist.

Vorgehensweise

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv6/conf/*/autoconf | egrep "default|all"` aus, um zu überprüfen, ob das Host-System autoconf-Einstellungen für IPv6 Router-Advertisements ablehnt.
- 2 Wenn diese Werte nicht auf 0 festgelegt sind, konfigurieren Sie das Host-System so, dass autoconf-Einstellungen der IPv6 Router-Advertisements abgelehnt werden.
 - a Öffnen Sie die Datei `/etc/sysctl.conf`.
 - b Wenn die Werte nicht auf 0 festgelegt sind, fügen Sie die folgenden Einträge zur Datei hinzu, oder aktualisieren Sie die vorhandenen Einträge entsprechend. Legen Sie den Wert auf 0 fest.


```
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.default.autoconf=0
```
 - c Speichern Sie die Änderungen, und schließen Sie die Datei.

Host-System so konfigurieren, dass IPv6 Nachbaranfragen abgelehnt werden

Prüfen Sie als Best Practice für die Sicherheit, dass das Host-System IPv6 Nachbaranfragen (Neighbor Solicitations) ablehnt, sofern diese nicht erforderlich sind. Die Einstellung `dad_transmits` bestimmt, wie viele Nachbaranfragen pro Adresse, einschließlich globaler und link-lokaler Adressen, gesendet werden, wenn Sie eine Schnittstelle starten, um sicherzustellen, dass die gewünschte Adresse im Netzwerk eindeutig ist.

Vorgehensweise

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv6/conf/*/dad_transmits | grep "default|all"` aus, um zu überprüfen, ob das Host-System IPv6 Nachbaranfragen ablehnt.
- 2 Wenn diese Werte nicht auf 0 festgelegt sind, konfigurieren Sie das Host-System so, dass IPv6 Nachbaranfragen abgelehnt werden.
 - a Öffnen Sie die Datei `/etc/sysctl.conf`.
 - b Wenn die Werte nicht auf 0 festgelegt sind, fügen Sie die folgenden Einträge zur Datei hinzu, oder aktualisieren Sie die vorhandenen Einträge entsprechend. Legen Sie den Wert auf 0 fest.


```
net.ipv6.conf.all.dad_transmits=0
net.ipv6.conf.default.dad_transmits=0
```
 - c Speichern Sie die Änderungen, und schließen Sie die Datei.

Host-System so konfigurieren, dass IPv6-Maximaladressen eingeschränkt werden

Als Best Practice für die Sicherheit müssen Sie überprüfen, ob der Host die Höchstzahl der IPv6-Adressen, die zugewiesen werden können, einschränkt. Die Einstellung der Maximaladressen bestimmt, wie viele globale IPv6-Unicast-Adressen jeder Schnittstelle zugewiesen werden können. Der Standardwert ist 16, aber Sie müssen die Anzahl auf die statistisch konfigurierten globalen Adressen festlegen, die erforderlich sind.

Vorgehensweise

- 1 Führen Sie den Befehl `# grep [1] /proc/sys/net/ipv6/conf/*/max_addresses | grep "default|all"` aus, um zu überprüfen, ob der Host die Höchstzahl der IPv6-Adressen, die zugewiesen werden können, einschränkt.
- 2 Wenn die Werte nicht auf 1 festgelegt sind, konfigurieren Sie das Host-System, um die Höchstzahl der IPv6-Adressen, die zugewiesen werden können, einzuschränken.
 - a Öffnen Sie die Datei `/etc/sysctl.conf`.
 - b Fügen Sie die folgenden Einträge zur Datei hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend. Legen Sie den Wert auf 1 fest.


```
net.ipv6.conf.all.max_addresses=1
net.ipv6.conf.default.max_addresses=1
```
 - c Speichern Sie die Änderungen, und schließen Sie die Datei.

Ports und Protokolle konfigurieren

Deaktivieren Sie als Best Practice für die Sicherheit alle nicht erforderlichen Ports und Protokolle.

Konfigurieren Sie ein Minimum an eingehenden und ausgehenden Ports für vRealize Operations Manager-Komponenten wie erforderlich, damit wichtige Systemkomponenten funktionieren.

Minimale Anzahl standardmäßiger eingehender Ports

Konfigurieren Sie als Best Practice für die Sicherheit die eingehenden Ports, die für den Betrieb von vRealize Operations Manager in der Produktion erforderlich sind.

Tabelle 4-1. Minimale Anzahl erforderlicher eingehender Ports

Port	Protokoll	Anmerkungen
443	TCP	Wird für den Zugriff auf die vRealize Operations Manager-Benutzeroberfläche und die vRealize Operations Manager-Verwaltungsschnittstelle verwendet.
123	UDP	Wird von vRealize Operations Manager für die NTP-Synchronisierung mit dem Master-Knoten verwendet.
5433	TCP	Wird von den Master- und Replikat-Knoten verwendet, um die globale Datenbank (vPostgreSQL) zu replizieren, wenn Hochverfügbarkeit aktiviert ist.
7001	TCP	Wird von Cassandra für eine sichere knotenübergreifende Cluster-Kommunikation verwendet. Achten Sie darauf, dass dieser Port im Internet nicht sichtbar ist. Fügen Sie diesen Port zu einer Firewall hinzu.
9042	TCP	Wird von Cassandra für sichere Client-bezogene Kommunikation zwischen den Knoten verwendet. Achten Sie darauf, dass dieser Port im Internet nicht sichtbar ist. Fügen Sie diesen Port zu einer Firewall hinzu.
6061	TCP	Wird von Clients verwendet, um eine Verbindung zu GemFire Locator aufzubauen und Verbindungsinformationen für Server im verteilten System abzurufen. Überwacht außerdem die Serverauslastung, um Clients zu den Servern mit der geringsten Auslastung zu senden.
10000-10010	TCP und UDP	Flüchtiger Portbereich des GemFire Server, der in einem verteilten Peer-to-Peer-System für Unicast-UDP-Messaging und zur TCP-Fehlererkennung verwendet wird.
20000-20010	TCP und UDP	Flüchtiger Portbereich des GemFire Locator, der in einem verteilten Peer-to-Peer-System für Unicast-UDP-Messaging und zur TCP-Fehlererkennung verwendet wird.

Tabelle 4-2. Optionale eingehende Ports

Port	Protokoll	Anmerkungen
22	TCP	Optional. Secure Shell (SSH). Der SSH-Service, der Port 22 oder einen anderen Port überwacht, muss in einer Produktionsumgebung deaktiviert werden, und Port 22 muss geschlossen werden.
80	TCP	Optional. Leiter zu 443 weiter.
3091-3101	TCP	Wenn Horizon View installiert ist, für den Zugriff auf Daten für vRealize Operations Manager von Horizon View verwendet.

Überwachung und Protokollierung auf Ihrem vRealize Operations Manager - System

5

Richten Sie als Best Practice für die Sicherheit die Überwachung und Protokollierung auf Ihrem vRealize Operations Manager-System ein.

Die detaillierte Implementierung der Überwachung und Protokollierung ist nicht Teil dieses Dokuments.

Remote-Protokollierung auf einem zentralen Protokoll-Host bietet einen sicheren Speicher für Protokolle. Durch das Speichern der Protokolldateien auf einem zentralen Host können Sie die Umgebung mit einem einzigen Tool problemlos überwachen. Außerdem können Sie aggregierte Analysen durchführen und nach koordinierten Angriffen auf mehrere Entitäten innerhalb der Infrastruktur suchen. Die Protokollierung auf einem sicheren, zentralisierten Protokollserver kann Protokollmanipulationen verhindern und dient außerdem als langfristiger Audit-Datensatz.

Dieses Kapitel behandelt die folgenden Themen:

- [„Sichern des Remote Logging-Servers“](#), auf Seite 55
- [„Autorisierten NTP-Server verwenden“](#), auf Seite 55
- [„Überlegungen zum Client-Browser“](#), auf Seite 56

Sichern des Remote Logging-Servers

Stellen Sie als Best Practice für die Sicherheit sicher, dass der Remote Logging-Server nur von einem autorisierten Benutzer konfiguriert werden kann und dass er sicher ist.

Angrifer, die die Sicherheit Ihres Host-Computers verletzen, könnten nach Protokolldateien suchen und diese manipulieren, um ihre Spuren zu verwischen und die Kontrolle zu behalten, ohne entdeckt zu werden.

Autorisierten NTP-Server verwenden

Stellen Sie sicher, dass alle Host-Systeme dieselben relativen Zeitquellen verwenden, einschließlich des relevanten Lokalisierungs-Offsets. Sie können die relative Zeitquelle mit einem vereinbarten Zeitstandard wie beispielsweise Coordinated Universal Time (UTC) korrelieren.

In den relevanten Protokolldateien können Sie die Aktionen eines Eindringlings problemlos verfolgen und korrelieren. Falsche Zeiteinstellungen könnten das Überprüfen und Korrelieren der Protokolldateien erschweren und zu einer falschen Überprüfung führen. Sie können mindestens drei NTP-Server von Zeitquellen außerhalb verwenden oder einige lokale NTP-Server auf einem vertrauenswürdigen Netzwerk konfigurieren, die ihre Zeit von mindestens drei Zeitquellen außerhalb beziehen.

Überlegungen zum Client-Browser

Verwenden Sie als Best Practice für die Sicherheit vRealize Operations Manager nicht von nicht vertrauenswürdigen oder nicht gepatchten Clients oder von Clients, die Browsererweiterungen verwenden.

Index

A

Administratorkonten **15**
Agentenressource entfernen **39**
Agentenressource wieder einsetzen **40**
Aktivitäten für eine sichere Konfiguration **41**
Aktualisieren von Zertifikaten **41**
Anwendungsressourcen, schützen **27**
Apache HTTPD **24**
Apache-Konfiguration **29**
Auf Linux installierte Bereitstellung **34**
autorisierter NTP-Server **55**

B

Beispielcode entfernen:Apache2-Server **29**
Benutzerkontrolle verhindern **43**
Best Practices, End Point Operations Management-Agenten **36**
Bestand der unterstützten Software **10**
Bluetooth-Protokoll-Handler **30**
Boot Loader-Authentifizierung **20**

C

Cipher-Suites in Apache HTTPD **26**
Cipher-Suites in GemFire **26**
Client-Konfiguration, Secure Shell **19**

D

Datagram Congestion Control Protocol **31**
Dateizugriffsberechtigungen, Secure Shell **17**
Daten während der Übertragung **24, 34**
deaktivieren, unnötige Anwendungen **41**
DECnet-Protokoll, sichern **33**
Diffie-Hellman **35**
Direktanmeldungen deaktivieren **19**
Drittanbietersoftware **10**
Durchsuchen deaktivieren **29**
Durchsuchen von Verzeichnissen deaktivieren **29**

E

Einzelnutzerauthentifizierung **20**
End Point Operations Management-Agent **35**

F

FIPS 140-2 Modus aktivieren **23**

G

GemFire-TLS-Handler-Protokolle **24**
Glossar **5**

H

Härten der Linux-Installation **10**
Härten der vSphere-Umgebung **10**
Härtung der Infrastruktur **9**
Hop-Limit-Einstellungen der IPv6 Router-Advertisements ablehnen **51**

I

ICMPv4 Echos für Broadcast-Adressen ablehnen **44**
Infrastruktur, Härtung **9**
installierte Software überprüfen **10**
IPv4 Source Routed-Pakete **47**
IPv4, 1Pv4-Weiterleitung ablehnen **47**
IPv4, ICMP Redirect-Meldungen ignorieren **45**
IPv4, IPv4 ICMP-Umleitungen ablehnen **46**
IPv4, IPv4 Reverse Path-Filterung ignorieren **46**
IPv4, IPv4 TCP Syncookies verwenden **48**
IPv4, IPv4-Martian-Pakete protokollieren **46**
IPv4, Proxy ARP deaktivieren **44**
IPv6 autoconf-Einstellungen **51**
IPv6 Router-Einstellungen ablehnen **51**
IPv6, ICMP Redirect-Meldungen ignorieren **45**
IPv6, IPv6 Nachbaranfragen ablehnen **52**
IPv6, IPv6 Router-Advertisements ablehnen **49**
IPv6, IPv6 Router-Anfragen ablehnen **49**
IPv6, IPv6 Router-Einstellungen bei Router-Anfragen ablehnen **50**
IPv6, IPv6 Router-Präfixe ablehnen **50**
IPv6, IPv6-Maximaladressen einschränken **52**
IPv6, IPv6-Weiterleitung ablehnen **48**

K

Kennwortablauf **15**
Kernel-Meldungsprotokollierung **33**
Konfiguration, PostgreSQL-Client-Authentifizierung **28**
Konfigurationsmodi, deaktivieren **30, 35**
konfigurieren **31, 52**
Konsole sichern **14**
Konsolenzugriff **15**

Llokales Administratorkonto, erstellen **16****M**

Minimal erforderliche Gruppen **21**
 Minimal erforderliche Gruppen überwachen **21**
 Minimale Anzahl eingehender Ports **53**
 Minimale Benutzerkonten **21**
 Minimale Benutzerkonten überwachen **21**
 Minimale Berechtigungen, Agentenfunktionalität **36**

N

Network Time Protocol **34**
 Network Time Protocol konfigurieren **22**
 Netzwerkeinstellungen **43**
 Netzwerkeinstellungen für OVF konfigurieren **43**

OOVF, Netzwerkeinstellungen **43****P**

Patches **41**
 Plattformdateien und Berechtigungen, Linux **36**
 Plattformdateien und Berechtigungen, Windows **37**
 Ports auf Agenten-Host öffnen **39**
 Ports und Protokolle, konfigurieren **31, 52**
 Protokollierung **55**

R

Remote Logging-Server > Sichern **55**
 Remote Logging-Server sichern **55**
 Root-Benutzer, Secure Shell **15**
 Root-Kennwort, ändern **14**
 Rückruf des Agentenzertifikats **41**

S

Schnittstellen
 ausgehend **43**
 eingehend **43**
 schwache Verschlüsselungen **35**
 schwache Verschlüsselungen, konfigurieren **34**
 Secure Shell, Einschränken des Zugriffs **17**
 Secure Shell-Client-Konfiguration **19**
 Secure Shell-Dateizugriffsberechtigungen **17**
 Secure Shell-Serverkonfiguration **18**
 Secure Shell, verwalten **15**
 Serverkonfiguration, Secure Shell **18**
 sichere Bereitstellung von vRealize Operations Manager **9**
 Sichere Konfiguration **13**
 sichere Konfiguration des Hostservers **35**

Sicherheitsaufstellung **7**Sicherheitsratgeber, Patches **11**

sichern

 Appletalk-Protokoll **32**
 Firewire-Modul **33**
 Internet Packet Exchange-Protokoll **32**
 Reliable Datagram Sockets-Protokoll **31**
 Transparent Inter-Process Communication-Protokoll **32**

SSH-Zugriff für das Admin-Benutzerkonto deaktivieren **20**Starke Protokolle **34**Starke Protokolle konfigurieren **34**starke Protokolle, konfigurieren **24**starke Verschlüsselungen **34**starke Verschlüsselungen, konfigurieren **25**Stream Control Transmission Protocol **31****T**TCP Zeitstempel-Response deaktivieren **23**TLS für Daten während der Übertragung **24, 34**Trace-Methode deaktivieren:Apache2-Server **30****U**Überlegungen zu Browsern **56**Überprüfen, Benutzerkontoeinstellungen des Servers **41**Überprüfen der Installationsmedien **9**Überprüfen von Server-Token:Apache2-Server **29**Überwachung **55**unnötige Anwendungen, löschen **41**unnötige Dienste deaktivieren **42**unnötige Ports deaktivieren **42**Updates **41**USB-Massenspeicher-Handler **30****V**Verwalten unwichtiger Software **30**

Virtuelle Appliances

 Bluetooth-Protokoll-Handler **30** Boot Loader-Authentifizierung **20** Network Time Protocol konfigurieren **22** Secure Shell aktivieren oder deaktivieren **16** USB-Massenspeicher-Handler **30**virtuelle Computer, IPv4 Proxy ARP deaktivieren **44**virtuelle Computer, ICMPv4 Echos für Broadcast-Adressen ablehnen **44**vRealize Operations Manager-Administrator-kennwort **22**

W

Warteschlangengröße für TCP-Backlog **43**

Wartungsmodus-Authentifizierung **20**

Weiterleitung ablehnen **47**

Widerrufen eines Agenten **39**

Z

Zielgruppe **5**

Zurücksetzen des Kennworts auf Linux-Clustern **22**

