

Handbuch zur sicheren Konfiguration

24. Oktober 2019

vRealize Automation 7.6



vmware®

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

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

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie diese an:

docfeedback@vmware.com

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Willy-Brandt-Platz 2
81829 München
Germany
Tel.: +49 (0) 89 3706 17 000
Fax: +49 (0) 89 3706 17 333
www.vmware.com/de

Copyright © 2015–2019 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

1	Sichere Konfiguration	5
2	Sichere Baseline für vRealize Automation – Übersicht	6
3	Überprüfen der Integrität der Installationsmedien	8
4	Härtung der Softwareinfrastruktur für VMware-Systeme	9
	Härtung der VMware vSphere ® -Umgebung	9
	Härtung des Infrastructure as a Service-Hosts	9
	Härtung von Microsoft SQL Server	10
	Härtung von Microsoft .NET	10
	Härtung der Microsoft Internetinformationsdienste (IIS)	10
5	Überprüfen der installierten Software	12
6	Empfehlungen und Patches für die Sicherheit von VMware	13
7	Sichere Konfiguration	14
	Sichern der vRealize Automation-Appliance	14
	Ändern des Root-Kennworts	14
	Überprüfen des Root-Kennworthash und der Komplexität	15
	Überprüfen des Root-Kennwortverlaufs	15
	Verwalten des Kennwortablaufs	16
	Verwalten von Secure Shell und Administratorkonten	17
	Ändern des Benutzers der Verwaltungsschnittstelle für die virtuelle Appliance	21
	Festlegen der Bootloader-Authentifizierung	22
	Konfigurieren von NTP	23
	Konfigurieren von TLS für übertragene Daten der vRealize Automation-Appliance	23
	Überprüfen der Sicherheit von Data-at-Rest	32
	Konfigurieren von vRealize Automation-Anwendungsressourcen	33
	Anpassen der Konsolen-Proxykonfiguration	36
	Konfigurieren von Server-Antwortkopfzeilen	38
	Festlegen der Zeitüberschreitung für eine vRealize Automation-Appliance-Sitzung	40
	Verwalten nicht erforderlicher Software	40
	Sichern der Infrastructure as a Service-Komponente	44
	Konfigurieren von NTP	44
	Konfigurieren von TLS für Infrastructure as a Service-Data-In-Transit	45
	Konfigurieren von TLS-Verschlüsselungs-Suites	48

Überprüfen der Hostserver-Sicherheit	49
Schützen von Anwendungsressourcen	50
Sichern der Infrastructure as a Service-Hostmaschine	51

8 Konfigurieren der Hostnetzwerksicherheit 52

Konfigurieren von Netzwerkeinstellungen für VMware-Appliances	52
Verhindern der Benutzerkontrolle von Netzwerkschnittstellen	52
Festlegen der Warteschlangengröße für TCP-Backlogs	53
Verweigern von ICMPv4-Echos für Broadcast-Adressen	53
Deaktivieren von IPv4 Proxy ARP	54
Verweigern von IPv4-ICMP-Umleitungsmeldungen	54
Verweigern von IPv6-ICMP-Umleitungsmeldungen	55
Protokollieren von IPv4-Martian-Paketen	56
Verwenden der IPv4 Reverse Path-Filterung	56
Verweigern der IPv4-Weiterleitung	57
Verweigern der IPv6-Weiterleitung	58
Verwenden von IPv4-TCP Syncookies	59
Verweigern von IPv6-Routerankündigungen	59
Verweigern von IPv6-Routeranfragen	60
Verweigern der IPv6 Routereinstellungen bei Routeranfragen	61
Verweigern von IPv6-Routerpräfixinformationen	62
Verweigern der Hop-Limit-Einstellungen bei IPv6-Routerankündigungen	62
Verweigern der Autoconf-Einstellungen von IPv6-Routerankündigungen	63
Verweigern von IPv6-Nachbaranfragen	64
Einschränken der maximalen Anzahl der IPv6-Adressen	64
Konfigurieren von Netzwerkeinstellungen für den Infrastructure as a Service-Host	65
Konfigurieren von Ports und Protokollen	65
Für Benutzer erforderliche Ports	66
Für Administrator erforderliche Ports	66

9 Überwachung und Protokollierung 70

Sichere Konfiguration

Mit der Funktion für sichere Konfiguration können Benutzer die sichere Konfiguration von vRealize Automation bewerten und optimieren.

Sichere Konfiguration beschreibt die Überprüfung und Konfiguration von sicheren Bereitstellungen für typische vRealize Automation-Umgebungen und bietet Informationen und Anweisungen, damit Benutzer fundierte Entscheidungen bezüglich der Sicherheitskonfiguration treffen können.

Zielgruppe

Diese Informationen richten sich an vRealize Automation-Systemadministratoren und andere Benutzer, die für die Sicherheit und Konfiguration des Systems zuständig sind.

VMware Technical Publications - Glossar

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

Sichere Baseline für vRealize Automation – Übersicht

2

VMware bietet umfassende Empfehlungen für das Überprüfen und Konfigurieren einer sicheren Baseline für Ihr vRealize Automation-System.

Verwenden Sie die von VMware angegebenen Tools und Verfahren, um eine gehärtete Baseline-Konfiguration für Ihr vRealize Automation-System zu erhalten. Einige vRealize Automation-Komponenten werden auf einer gehärteten bzw. teilweise gehärteten Basis installiert. Unter Berücksichtigung der VMware-Sicherheitsempfehlungen, Unternehmenssicherheitsrichtlinien und bekannten Bedrohungen sollten Sie jedoch alle Komponenten überprüfen und bestätigen.

vRealize Automation-Sicherheitsniveau

Das Sicherheitsniveau von vRealize Automation geht von einer ganzheitlich sicheren Umgebung basierend auf der System- und Netzwerkkonfiguration, den Sicherheitsrichtlinien des Unternehmens und den Best Practices zur Sicherheit aus.

Wenn Sie die Härtung eines vRealize Automation-Systems überprüfen und konfigurieren, beachten Sie die VMware-Empfehlungen zur Härtung in den folgenden Bereichen.

- Sichere Bereitstellung
- Sichere Konfiguration
- Netzwerksicherheit

Um sicherzustellen, dass Ihr System gehärtet ist, überprüfen Sie die VMware-Empfehlungen und Ihre lokalen Sicherheitsrichtlinien, da diese sich auf die genannten konzeptionellen Bereiche beziehen.

Systemkomponenten

Stellen Sie für die Härtung und sichere Konfiguration Ihres vRealize Automation-Systems sicher, dass Sie die Funktionsweise aller Komponenten und ihr Zusammenspiel hinsichtlich der Unterstützung der Systemfunktionalität kennen.

Beachten Sie bei der Planung und Implementierung eines sicheren Systems die folgenden Komponenten.

- vRealize Automation-Appliance
- IaaS-Komponente

Wenn Sie sich mit vRealize Automation und dem Zusammenspiel der Komponenten vertraut machen möchten, finden Sie hilfreiche Informationen unter *Grundlagen und Konzepte* im VMware vRealize Automation-Dokumentationscenter. Informationen zu den typischen Bereitstellungen und der Architektur von vRealize Automation finden Sie in der *Referenzarchitektur*. Eine Dokumentation finden Sie unter [Dokumentation zu VMware vRealize Automation](#).

Überprüfen der Integrität der Installationsmedien

3

Benutzer sollten vor der Installation eines VMware-Produkts immer die Integrität der Installationsmedien überprüfen.

Überprüfen Sie nach dem Download eines ISO-Images, Offline-Pakets oder Patches stets den SHA1-Hashwert, um die Integrität und Authentizität der heruntergeladenen Dateien sicherzustellen. Wenn Sie physische Medien von VMware erhalten und das Sicherheitssiegel beschädigt ist, schicken Sie die Software an VMware zurück, um Ersatz zu erhalten.

Nach dem Herunterladen der Medien überprüfen Sie mithilfe des MD5/SHA1-Summenwerts die Integrität des Downloads. Vergleichen Sie die ausgegebene MD5/SHA1-Summe mit dem auf der VMware-Website angegebenen Wert. SHA1- oder MD5-Hashwert müssen übereinstimmen.

Weitere Informationen zum Überprüfen der Integrität der Installationsmedien finden Sie unter <http://kb.vmware.com/kb/1537>.

Härtung der Softwareinfrastruktur für VMware-Systeme

4

Bewerten Sie im Rahmen der Härtung die bereitgestellte Softwareinfrastruktur, die Ihr VMware-System unterstützt, und stellen Sie sicher, dass die Richtlinien zur Härtung von VMware eingehalten werden.

Überprüfen Sie vor der Härtung Ihres VMware-Systems die unterstützende Softwareinfrastruktur und beheben Sie mögliche Sicherheitsschwachstellen, um eine vollständig gehärtete Umgebung einzurichten. Bei den möglichen Softwareinfrastruktur-Elementen handelt es sich um Betriebssystemkomponenten, unterstützende Software und Datenbanksoftware. Räumen Sie Sicherheitsbedenken bei diesen und anderen Komponenten entsprechend den Empfehlungen des Herstellers und anderen relevanten Sicherheitsprotokollen aus.

Dieses Kapitel enthält die folgenden Themen:

- [Härtung der VMware vSphere® -Umgebung](#)
- [Härtung des Infrastructure as a Service-Hosts](#)
- [Härtung von Microsoft SQL Server](#)
- [Härtung von Microsoft .NET](#)
- [Härtung der Microsoft Internetinformationsdienste \(IIS\)](#)

Härtung der VMware vSphere® -Umgebung

Bewerten Sie die VMware vSphere® -Umgebung und stellen Sie sicher, dass ein angemessener Grad an vSphere-Härtung durchgesetzt und aufrecht erhalten wird.

Weitere Informationen zur Härtung finden Sie unter <http://www.vmware.com/security/hardening-guides.html>.

Im Rahmen einer umfassend gehärteten Umgebung muss die VMware vSphere® -Infrastruktur den in VMWaredefinierten Sicherheitsrichtlinien entsprechen.

Härtung des Infrastructure as a Service-Hosts

Stellen Sie sicher, dass Ihre Infrastructure as a Service-Hostmaschine unter Microsoft Windows gemäß der VMware-Richtlinien gehärtet ist.

Überprüfen Sie die Empfehlungen in den jeweiligen von Microsoft Windows empfohlenen Richtlinien zur Härtung und stellen Sie sicher, dass Ihr Windows Server-Host entsprechend gehärtet ist. Wenn Sie die Empfehlungen zur Härtung nicht befolgen, kann dies zur Offenlegung von bekannten Sicherheitsschwachstellen über unsichere Komponenten von Windows-Versionen führen.

Informationen darüber, ob Ihre Version unterstützt wird, finden Sie in der [Support-Matrix für vRealize Automation Support](#).

Wenden Sie sich an Ihren Microsoft-Anbieter und fordern Sie Unterstützung bei der Härtung von Microsoft-Produkten an.

Härtung von Microsoft SQL Server

Stellen Sie sicher, dass die Microsoft SQL Server-Datenbank die von Microsoft und VMware festgelegten Sicherheitsrichtlinien einhält.

Überprüfen Sie die Empfehlungen in den entsprechenden Best Practice-Richtlinien zur Härtung und Sicherheit von Microsoft SQL Server. Überprüfen Sie alle Microsoft-Sicherheitsbulletins im Hinblick auf die installierte Version von Microsoft SQL Server. Wenn Sie die Empfehlungen zur Härtung nicht befolgen, kann dies zur Offenlegung von bekannten Sicherheitsschwachstellen über unsichere Komponenten von Microsoft SQL Server-Versionen führen.

Informationen darüber, ob Ihre Version von Microsoft SQL Server unterstützt wird, finden Sie in der [Support-Matrix für vRealize Automation](#).

Wenden Sie sich an Ihren Microsoft-Anbieter und fordern Sie Unterstützung beim Härten von Microsoft-Produkten an.

Härtung von Microsoft .NET

Im Rahmen einer umfassend gehärteten Umgebung muss Microsoft .NET die von Microsoft und VMware vorgeschriebenen Sicherheitsrichtlinien einhalten.

Überprüfen Sie die Empfehlungen in den entsprechenden Best Practice-Richtlinien zur Härtung und Sicherheit von .NET. Überprüfen Sie alle Microsoft-Sicherheitsbulletins im Hinblick auf die von Ihnen verwendete Version von Microsoft SQL Server. Wenn Sie die Empfehlungen zur Härtung nicht befolgen, kann dies zur Offenlegung von bekannten Sicherheitsschwachstellen über unsichere Microsoft.NET-Komponenten führen.

Informationen darüber, ob Ihre Version von Microsoft.NET unterstützt wird, finden Sie in der [Support-Matrix für vRealize Automation](#).

Wenden Sie sich an Ihren Microsoft-Anbieter und fordern Sie Unterstützung beim Härten von Microsoft-Produkten an.

Härtung der Microsoft Internetinformationsdienste (IIS)

Stellen Sie sicher, dass Ihre Microsoft Internetinformationsdienste (IIS) alle von Microsoft und VMware vorgegebenen Sicherheitsrichtlinien einhalten.

Überprüfen Sie die Empfehlungen in den entsprechenden Best Practice-Richtlinien zur Härtung und Sicherheit von Microsoft IIS. Überprüfen Sie alle Microsoft-Sicherheitsbulletins im Hinblick auf die von Ihnen verwendete Version von IIS. Wenn Sie die Empfehlungen zur Härtung nicht befolgen, kann das zum Auftreten von bekannten Sicherheitsschwachstellen führen.

Informationen darüber, ob Ihre Version unterstützt wird, finden Sie in der [Support-Matrix für vRealize Automation Support](#).

Wenden Sie sich an Ihren Microsoft-Anbieter und fordern Sie Unterstützung beim Härten von Microsoft-Produkten an.

Überprüfen der installierten Software

5

Da Schwachstellen in Software von Drittanbietern und nicht verwendeter Software das Risiko eines nicht autorisierten Systemzugriffs erhöhen und zu Unterbrechungen der Verfügbarkeit führen können, sollten Sie die gesamte auf den VMware-Hostmaschinen installierte Software überprüfen und ihre Verwendung bewerten.

Installieren Sie keine Software, die für den sicheren Betrieb des Systems auf den VMware-Hostmaschinen nicht erforderlich ist. Deinstallieren Sie nicht verwendete oder irrelevante Software.

In der Bestandsliste installierte nicht unterstützte Software

Bewerten Sie die VMware-Bereitstellung und den Bestand der installierten Produkte, um sicherzustellen, dass keine überflüssige nicht unterstützte Software installiert ist.

Weitere Informationen zu den Supportrichtlinien für Drittanbieterprodukte finden Sie im VMware Supportartikel unter <https://www.vmware.com/support/policies/thirdparty.html>.

Überprüfen von Drittanbietersoftware

VMware unterstützt oder empfiehlt nicht die Installation von Drittanbietersoftware, die nicht getestet und bestätigt wurde. Unsichere, nicht gepatchte oder nicht authentifizierte Drittanbietersoftware, die auf VMware-Hostmaschinen installiert ist, kann das System dem Risiko des unerlaubten Zugriffs aussetzen und zu Unterbrechungen der Verfügbarkeit führen. Wenn Sie nicht unterstützte Drittanbietersoftware verwenden müssen, wenden Sie sich an den Drittanbieter und informieren Sie sich über die Konfigurations- und Patching-Anforderungen.

Empfehlungen und Patches für die Sicherheit von VMware

6

Um die größtmögliche Sicherheit für Ihr System beizubehalten, beachten Sie die VMware-Sicherheitsempfehlungen und wenden Sie alle relevanten Patches an.

VMware hat Sicherheitsempfehlungen für Produkte veröffentlicht. Beachten Sie die Empfehlungen, um sicherzustellen, dass Ihr Produkt vor bekannten Bedrohungen geschützt ist.

Bewerten Sie die Installation, den Patch-Vorgang und den Upgrade-Verlauf von vRealize Automation und stellen Sie sicher, dass die veröffentlichten VMware-Sicherheitsempfehlungen befolgt und durchgesetzt werden.

Weitere Informationen zu den aktuellen VMware-Sicherheitsempfehlungen finden Sie unter <http://www.vmware.com/security/advisories/>.

Sichere Konfiguration

Überprüfen und aktualisieren Sie die Sicherheitseinstellungen für virtuelle vRealize Automation-Appliances und die Infrastructure as a Service-Komponente gemäß den Anforderungen Ihrer Systemkonfiguration. Überprüfen und aktualisieren Sie darüber hinaus weitere Komponenten oder Anwendungen.

Die sichere Konfiguration einer vRealize Automation-Installation umfasst die Konfiguration jeder einzelnen Komponente, da alle Komponenten ein funktionierendes Ganzes bilden. Konfigurieren Sie alle Systemkomponenten in Abstimmung zueinander, um eine angemessene sichere Baseline zu erreichen.

Dieses Kapitel enthält die folgenden Themen:

- [Sichern der vRealize Automation-Appliance](#)
- [Sichern der Infrastructure as a Service-Komponente](#)

Sichern der vRealize Automation-Appliance

Überprüfen und aktualisieren Sie die Sicherheitseinstellungen für die vRealize Automation-Appliance wie für die Systemkonfiguration erforderlich.

Konfigurieren Sie die Sicherheitseinstellungen für Ihre virtuellen Appliances und deren Hostbetriebssysteme. Legen Sie darüber hinaus die Konfiguration anderer zugehöriger Komponenten und Anwendungen fest oder überprüfen Sie sie. In einigen Fällen müssen Sie vorhandene Einstellungen überprüfen, während Sie für andere Einstellungen ändern oder hinzufügen müssen, um eine entsprechende Konfiguration zu erreichen.

Ändern des Root-Kennworts

Sie können das Root-Kennwort für die vRealize Automation-Appliance ändern.

Verfahren

- 1 Melden Sie sich bei der Verwaltungsschnittstelle der vRealize Automation-Appliance als Root-Benutzer an.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Klicken Sie auf die Registerkarte **Administrator**.
- 3 Klicken Sie auf das Untermenü **Admin**.
- 4 Geben Sie das vorhandene Kennwort in das Textfeld **Aktuelles Administratorkennwort** ein.

- 5 Geben Sie das neue Kennwort in das Textfeld **Neues Administratorkennwort** ein.
- 6 Geben Sie das neue Kennwort in das Textfeld **Neues Administratorkennwort erneut eingeben** ein.
- 7 Klicken Sie auf **Einstellungen speichern**.

Überprüfen des Root-Kennworthash und der Komplexität

Stellen Sie sicher, dass das Root-Kennwort die Komplexitätsanforderungen an Kennwörter in Ihrem Unternehmen erfüllt.

Das Überprüfen der Komplexität des Root-Kennworts ist erforderlich, da der Root-Benutzer die Komplexitätsprüfung des Kennworts mithilfe des pam_crackli-Moduls umgeht, das an Benutzerkonten angehängt ist.

Das Kennwort des Kontos muss mit \$6\$ beginnen, was einen sha512-Hashwert anzeigt. Dies ist der standardmäßige Hashwert für alle gehärteten Appliances.

Verfahren

- 1 Um den Hashwert des Root-Kennworts zu überprüfen, melden Sie sich als Root-Benutzer an und führen den Befehl `# more /etc/shadow` aus.

Die Hashinformationen werden angezeigt.

Abbildung 7-1. Ergebnisse des Kennworthashes

```
vcac148-084-111:~ # more /etc/shadow
bin:!:16332:0:60:7:::
daemon:!:16332:0:60:7:::
haldaemon:!:16332:0:60:7:::
mail:!:15870::60:::
man:!:16332:0:60:7:::
messagebus:!:16332:0:60:7:::
nobody:!:15870::60:::
ntp:!:16332:0:60:7:::
polkituser:!:16332:0:60:7:::
postfix:!:16332:0:60:7:::
root:$6$PHxGPY5A$ba8KzK4SS44UEHPfAtgs
P/:16346:0:365:7:::
```

- 2 Wenn das Root-Kennwort keinen sha512-Hash enthält, führen Sie den `passwd`-Befehl aus, um ihn zu ändern.

Alle gehärteten Appliances verwenden `enforce_for_root` für das `pw_history`-Modul aus der Datei `etc/pam.d/common-password`. Standardmäßig speichert das System die letzten fünf Kennwörter. Alte Kennwörter werden für jeden Benutzer in der Datei `/etc/securetty/passwd` gespeichert.

Überprüfen des Root-Kennwortverlaufs

Stellen Sie sicher, dass der Kennwortverlauf für das Root-Konto durchgesetzt wird.

Alle gehärteten Appliances verwenden `enforce_for_root` für das `pw_history`-Modul aus der Datei `etc/pam.d/common-password`. Standardmäßig speichert das System die letzten fünf Kennwörter. Alte Kennwörter werden für jeden Benutzer in der Datei `/etc/securetty/passwd` gespeichert.

Verfahren

- 1 Führen Sie den folgenden Befehl aus:

```
cat /etc/pam.d/common-password-vmware.local | grep pam_pwhistory.so
```

- 2 Stellen Sie sicher, dass `enforce_for_root` in den zurückgegebenen Ergebnissen angezeigt wird.

```
password required pam_pwhistory.so enforce_for_root remember=5 retry=3
```

Verwalten des Kennwortablaufs

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

Standardmäßig verwenden alle Konten von gehärteten virtuellen VMware-Appliances einen Kennwortablauf von 60 Tagen. Auf den meisten gehärteten Appliances ist für das Root-Konto ein Kennwortablauf von 365 Tagen festgelegt. Überprüfen Sie im Sinne der Best Practice, dass die Ablaufzeit für alle Kontokennwörter sowohl die Sicherheits- als auch die Betriebsanforderungen erfüllt.

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

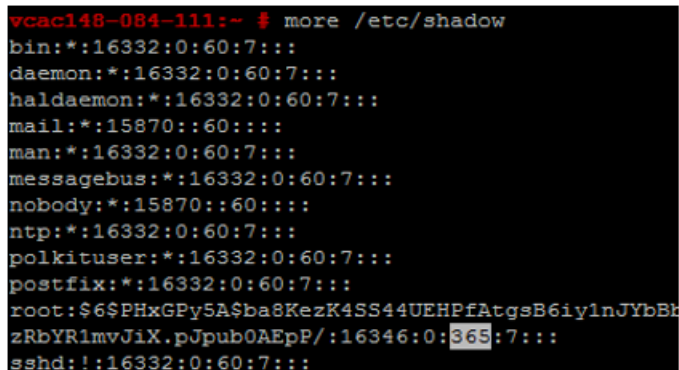
Verfahren

- 1 Melden Sie sich bei Ihren Maschinen mit virtuellen Appliances als Root-Benutzer an und führen Sie den folgenden Befehl aus, um den Kennwortablauf für alle Konten zu überprüfen.

```
# cat /etc/shadow
```

Der Kennwortablauf ist das fünfte Feld (Felder werden durch Doppelpunkte getrennt) der Shadow-Datei. Die Root-Ablaufdauer wird in Tagen festgelegt.

Abbildung 7-2. Feld „Kennwortablauf“



```
vcac148-084-111:~ $ more /etc/shadow
bin:!:16332:0:60:7:::
daemon:!:16332:0:60:7:::
haldaemon:!:16332:0:60:7:::
mail:!:15870::60:::
man:!:16332:0:60:7:::
messagebus:!:16332:0:60:7:::
nobody:!:15870::60:::
ntp:!:16332:0:60:7:::
polkituser:!:16332:0:60:7:::
postfix:!:16332:0:60:7:::
root:$6$PHxGPY5A$ba8KzK4SS44UEHPfAtgsB6iy1nJYbBt
zRbYR1mvJiX.pJpub0AEpP/:16346:0:365:7:::
sshd:!:16332:0:60:7:::
```

- 2 Um den Ablauf des Root-Kontos zu ändern, führen Sie einen Befehl im folgenden Format aus.

```
# passwd -x 365 root
```


In diesem Befehl gibt 365 die Anzahl der Tage bis zum Ablauf des Kennworts an. Verwenden Sie denselben Befehl, um beliebige Benutzer zu ändern. Ersetzen Sie dabei das spezifische Konto für 'root' und die Anzahl der Tage, sodass sie die Standards für den Kennwortablauf der Organisation erfüllen.

Verwalten von Secure Shell und Administratorkonten

Für Remoteverbindungen umfassen alle gehärteten Appliances das Secure Shell (SSH)-Protokoll. Verwenden Sie SSH nur bei Bedarf und verwalten Sie diese Befehlszeilenumgebung zur Erhaltung der Systemsicherheit.

SSH ist eine interaktive Befehlszeilenumgebung, die Remoteverbindungen zu virtuellen VMware-Appliances unterstützt. Standardmäßig erfordert der SSH-Zugriff die Anmeldedaten eines Benutzerkontos mit weitreichenden Berechtigungen. Bei SSH-Aktivitäten von Root-Benutzern werden die rollenbasierte Zugriffssteuerung (Role-Based Access Control, RBAC) und Überwachungssteuerung der virtuellen Appliance in der Regel umgangen.

Es wird empfohlen, SSH in einer Produktionsumgebung zu deaktivieren und nur dann zu aktivieren, wenn Probleme behoben werden müssen, die mit anderen Mitteln nicht behoben werden können. Lassen Sie SSH nur solange aktiviert, wie es für einen bestimmten Zweck erforderlich ist und wie es die Sicherheitsrichtlinien Ihres Unternehmens zulassen. SSH ist auf der vRealize Automation-Appliance standardmäßig deaktiviert. Je nach Ihrer vSphere-Konfiguration können Sie SSH aktivieren oder deaktivieren, wenn Sie Ihre OVF (Open Virtualization Format)-Vorlage bereitstellen.

Ein einfacher Test, um zu ermitteln, ob SSH auf einer Maschine aktiviert ist, besteht darin, zu versuchen, eine Verbindung unter Verwendung von SSH zu öffnen. Wenn die Verbindung geöffnet wird und Anmeldedaten abgefragt werden, ist SSH aktiviert und für Verbindungen verfügbar.

Secure Shell-Root-Benutzerkonto

Da VMware-Appliances keine vorkonfigurierten Benutzerkonten enthalten, kann SSH vom Root-Konto standardmäßig für eine direkte Anmeldung verwendet werden. Deaktivieren Sie SSH so schnell wie möglich als Boot-Benutzer.

Um die Übereinstimmungsstandards für Unleugbarkeit zu erfüllen, ist der SSH-Server auf allen gehärteten Appliances mit einem AllowGroups-Wheel-Eintrag vorkonfiguriert, um den SSH-Zugriff auf den sekundären Gruppen-Wheel-Eintrag einzuschränken. Um die Verantwortlichkeiten zu trennen, können Sie den AllowGroups-Wheel-Eintrag in der Datei `/etc/ssh/sshd_config` zwecks Verwendung einer anderen Gruppe, wie `sshd`, ändern.

Die Wheel-Gruppe ist mit dem `pam_wheel`-Modul für den Superuser-Zugriff aktiviert, sodass Mitglieder der Wheel-Gruppe `su-root` ausführen können, wenn das Root-Kennwort erforderlich ist. Eine Gruppentrennung ermöglicht Benutzern die Verwendung von SSH auf der Appliance, nicht aber die Ausführung von `su` auf `root`. Entfernen oder ändern Sie keine anderen Einträge im AllowGroups-Feld, um die ordnungsgemäße Funktionalität der Appliance sicherzustellen. Nach einer Änderung müssen Sie den SSH-Daemon neu starten, indem Sie diesen Befehl ausführen: `# service sshd restart`.

Aktivieren oder Deaktivieren von Secure Shell auf den vRealize Automation-Appliances

Aktivieren Sie Secure Shell (SSH) auf der vRealize Automation-Appliance nur zur Fehlerbehebung. Deaktivieren Sie SSH auf diesen Komponenten während des normalen Produktionsbetriebs.

Sie können SSH auf der vRealize Automation-Appliance mithilfe der Verwaltungsschnittstelle der vRealize Automation-Appliance aktivieren oder deaktivieren.

Verfahren

- 1 Melden Sie sich bei der Verwaltungsschnittstelle der vRealize Automation-Appliance als Root-Benutzer an.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Klicken Sie auf die Registerkarte **Administrator**.
- 3 Klicken Sie auf das Untermenü **Administrator**.
- 4 Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **SSH-Dienst zu aktivieren**, um SSH zu aktivieren bzw. zu deaktivieren.
- 5 Klicken Sie auf **Einstellungen speichern**, um Ihre Änderungen zu speichern.

Erstellen eines lokalen Administratorkontos für Secure Shell

Erstellen und konfigurieren Sie als Best Practice im Hinblick auf die Sicherheit lokale Administratorkonten für Secure Shell (SSH) auf den Hostmaschinen für virtuelle Appliances. Entfernen Sie auch den Root-SSH-Zugriff nach dem Erstellen der entsprechenden Konten.

Erstellen Sie lokale Administratorkonten für SSH oder Mitglieder der sekundären Wheel-Gruppe bzw. beides. Testen Sie vor dem Deaktivieren des direkten Root-Zugriffs, dass autorisierte Administratoren mit AllowGroups auf SSH zugreifen und mit der Wheel-Gruppe su auf root ausführen können.

Verfahren

- 1 Melden Sie sich bei der virtuellen Appliance als Root-Benutzer an und führen Sie die folgenden Befehle mit dem entsprechenden Benutzernamen aus.

```
# useradd -g users <username> -G wheel -m -d /home/benutzername
# passwd username
```

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

- 2 Wechseln Sie zum Benutzer und geben Sie ein neues Kennwort ein, um die Prüfung der Kennwortkomplexität zu erzwingen.

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

Wenn die Kennwortkomplexität erfüllt wird, wird das Kennwort aktualisiert. Wenn die Kennwortkomplexität nicht erfüllt wird, wird das Kennwort auf das ursprüngliche Kennwort zurückgesetzt, und Sie müssen den Kennwortbefehl erneut ausführen.

- 3 Um die direkte Anmeldung bei SSH zu entfernen, ändern Sie die Datei `/etc/ssh/sshd_config` durch Ersetzen von `(#)PermitRootLogin yes` durch `PermitRootLogin no`.

Alternativ dazu können Sie in der Virtual Appliance Management Interface (VAMI) SSH aktivieren/deaktivieren, indem Sie das Kontrollkästchen **Administrator-SSH-Anmeldung aktiviert** auf der Registerkarte **Admin** aktivieren bzw. deaktivieren.

Nächste Schritte

Deaktivieren Sie direkte Anmeldungen als Root-Benutzer. Standardmäßig erlauben die gehärteten Appliances die direkte Anmeldung als Root-Benutzer über die Konsole. Nachdem Sie Administratorkonten für die Unleugbarkeit erstellt und diese für den Su-Root-Wheel-Zugriff getestet haben, deaktivieren Sie direkte Root-Anmeldungen durch Bearbeiten der Datei `/etc/security` als Root-Benutzer und Ersetzen des `tty1`-Eintrags durch `console`.

- 1 Öffnen Sie die Datei `/etc/securetty` in einem Texteditor.
- 2 Suchen Sie `tty1` und ersetzen Sie es durch `console`.
- 3 Speichern Sie die Datei und schließen Sie sie.

Härten der Secure Shell-Serverkonfiguration

Sofern möglich, weisen alle VMware-Appliances eine standardmäßige gehärtete Konfiguration auf. Benutzer können die ausreichende Härtung ihrer Konfiguration überprüfen, indem Sie die Server- und Clienteneinstellungen im Abschnitt mit globalen Optionen der Konfigurationsdatei untersuchen.

Verfahren

- 1 Öffnen Sie die Konfigurationsdatei `/etc/ssh/sshd_config` auf der VMware-Appliance und stellen Sie sicher, dass die Einstellungen korrekt sind.

Einstellung	Status
Server-Daemon-Protokoll	Protokoll 2
CBC-Verschlüsselungen	aes256-ctr und aes128-ctr
TCP-Weiterleitung	AllowTCPForwarding Nein
Server-Gateway-Ports	Gateway-Ports Nein
X11-Weiterleitung	X11Forwarding, Nein
SSH-Dienst	Verwenden Sie das Feld „AllowGroups“ und geben Sie den zulässigen Zugriff für eine Gruppe an. Fügen Sie dieser Gruppe die passenden Mitglieder hinzu.
GSSAPI-Authentifizierung	GSSAPIAuthentication Nein, sofern nicht verwendet
Keberos-Authentifizierung	KeberosAuthentication Nein, sofern nicht verwendet

Einstellung	Status
Lokale Variablen (globale AcceptEnv-Option)	Auf deaktiviert durch Auskommentieren oder für LC_* oder LANG-Variablen aktiviert festlegen
Tunnel-Konfiguration	PermitTunnel Nein
Netzwerksitzungen	MaxSessions 1
Gleichzeitige Benutzerverbindungen	Für Root- und andere Benutzer auf 1 festlegen. Die Datei /etc/security/limits.conf muss auch mit derselben Einstellung konfiguriert werden.
Überprüfung des strengen Modus	Strenge Modi Ja
Berechtigungstrennung	UsePrivilegeSeparation Ja
Rhosts RSA-Authentifizierung	RhostsESAAuthentication 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-Clientkonfiguration

Bewerten Sie im Rahmen der Härtung Ihres Systems die Härtung des SSH-Clients, indem Sie die SSH-Clientkonfigurationsdatei auf den Hostmaschinen der virtuellen Appliance überprüfen und sicherstellen, dass die VMware-Richtlinien eingehalten werden.

Verfahren

- 1 Öffnen Sie die SSH-Clientkonfigurationsdatei /etc/ssh/ssh_config und stellen Sie sicher, dass die Einstellungen im Abschnitt mit den globalen Optionen korrekt sind.

Einstellung	Status
Clientprotokoll	Protokoll 2
Client-Gateway-Ports	Gateway-Ports Nein
GSSAPI-Authentifizierung	GSSAPIAuthentication Nein
Lokale Variablen (globale SendEnv-Option)	Nur LC_* oder LANG-Variablen angeben
CBC-Verschlüsselungen	nur aes256-ctr und aes128-ctr
Meldungsauthentifizierungscode	Nur im MACs hmac-sha1-Eintrag verwendet

2 Speichern Sie die Änderungen und schließen Sie die Datei.

Überprüfen von Berechtigungen für Secure Shell-Schlüsseldateien

Um die Wahrscheinlichkeit von Angriffen zu minimieren, behalten Sie kritische Berechtigungen für SSH-Schlüsseldateien auf den Hostmaschinen Ihrer virtuellen Appliances bei.

Stellen Sie nach dem Konfigurieren oder Aktualisieren Ihrer SSH-Konfiguration immer sicher, dass die folgenden Berechtigungen für SSH-Schlüsseldateien nicht geändert werden.

- Die Schlüsseldateien für öffentliche Hosts in `/etc/ssh/*key.pub` gehören dem Root-Benutzer, und die Berechtigungen für diese Dateien sind auf 0644 (-rw-r--r--) festgelegt.
- Die Schlüsseldateien für private Hosts in `/etc/ssh/*key` gehören dem Root-Benutzer, und die Berechtigungen für diese Dateien sind auf 0600 (-rw-----) festgelegt.

Überprüfen der SSH-Berechtigungen für Schlüsseldateien

Stellen Sie sicher, dass SSH-Berechtigungen auf öffentliche und private Schlüsseldateien angewendet werden.

Verfahren

- 1 Überprüfen Sie die öffentlichen SSH-Schlüsseldateien, indem Sie folgenden Befehl ausführen: `ls -l /etc/ssh/*key.pub`
- 2 Stellen Sie sicher, dass als Besitzer und Gruppenbesitzer Root festgelegt ist und dass die Berechtigungen für die Dateien auf 0644 (-rw-r--r--) festgelegt wurden.
- 3 Lösen Sie etwaige Probleme, indem Sie die folgenden Befehle ausführen.


```
chown root /etc/ssh/*key.pub
chgrp root /etc/ssh/*key.pub
chmod 644 /etc/ssh/*key.pub
```
- 4 Überprüfen Sie die privaten SSH-Schlüsseldateien, indem Sie folgenden Befehl ausführen: `ls -l /etc/ssh/*key`
- 5 Stellen Sie sicher, dass Besitzer und Gruppenbesitzer als Root fungieren und dass die Berechtigungen für die Dateien auf 0600 (-rw-----) festgelegt wurden. Lösen Sie etwaige Probleme, indem Sie die folgenden Befehle ausführen.


```
chown root /etc/ssh/*key
chgrp root /etc/ssh/*key
chmod 600 /etc/ssh/*key
```

Ändern des Benutzers der Verwaltungsschnittstelle für die virtuelle Appliance

Sie können Benutzer in der Verwaltungsschnittstelle der virtuellen Appliance hinzufügen und löschen, um für das gewünschte Maß an Sicherheit zu sorgen.

Das Root-Benutzerkonto für die Verwaltungsschnittstelle der virtuellen Appliance verwendet PAM für die Authentifizierung. Daher finden hier die Clipping-Ebenen von PAM Anwendung. Wenn Sie die Verwaltungsschnittstelle der virtuellen Appliance nicht ordnungsgemäß isoliert haben, kann das Root-Konto blockiert werden, wenn ein Angreifer versucht, eine Anmeldung zu erzwingen. Darüber hinaus können Sie den Admin-Benutzer für die Verwaltungsschnittstelle ändern, wenn mehrere Personen in Ihrer Organisation das Root-Konto für die Unleugbarkeit nicht für ausreichend halten.

Voraussetzungen

Verfahren

- 1 Führen Sie den folgenden Befehl aus, um einen neuen Benutzer zu erstellen und ihn zu der Verwaltungsschnittstellengruppe der virtuellen Appliance hinzuzufügen.

```
useradd -G vami,root Benutzer
```

- 2 Erstellen Sie ein Kennwort für den Benutzer.

```
passwd Benutzer
```

- 3 (Optional) Führen Sie den folgenden Befehl aus, um den Root-Zugriff auf die Verwaltungsschnittstelle der virtuellen Appliance zu deaktivieren.

```
usermod -R vami root
```

Hinweis Durch das Deaktivieren des Root-Zugriffs auf die Verwaltungsschnittstelle der virtuellen Appliance wird auch die Möglichkeit deaktiviert, den Administrator, den Root-Administrator oder das Kennwort über die Registerkarte Admin zu ändern.

Festlegen der Bootloader-Authentifizierung

Um einen angemessenen Grad an Sicherheit bereitzustellen, konfigurieren Sie Bootloader-Authentifizierung auf ihren virtuellen VMware-Appliances.

Wenn der Bootloader des Systems keine Authentifizierung erfordert, können Benutzer mit Zugriff auf die Systemkonsole die Konfiguration für das Starten des Systems ändern oder das System im Einzelbenutzer- oder Wartungsmodus starten, was zu einem Denial-of-Service oder zu nicht autorisiertem Zugriff führen kann. Da die Bootloader-Authentifizierung auf virtuellen VMware-Appliances nicht standardmäßig festgelegt ist, müssen Sie ein GRUB-Kennwort erstellen, um sie zu konfigurieren.

Verfahren

- 1 Überprüfen Sie, ob ein Boot-Kennwort vorhanden ist, indem Sie die `password --md5 <password-hash>`-Zeile der Datei `/boot/grub/menu.lst` auf Ihrer virtuellen Appliance suchen.
- 2 Wenn kein Kennwort vorhanden ist, führen Sie den `# /usr/sbin/grub-md5-crypt`-Befehl für Ihre virtuelle Appliance aus.

Ein MD5-Kennwort wird generiert, und der Befehl liefert die md5-Hash-Ausgabe.

- 3 Fügen Sie das Kennwort der Datei `menu.lst` an, indem Sie den `# password --md5 <hash from grub-md5-crypt>`-Befehl ausführen.

Konfigurieren von NTP

Für die kritische Zeitermittlung deaktivieren Sie die Hostzeitsynchronisierung und verwenden Sie das Network Time Protocol (NTP) auf der vRealize Automation-Appliance.

Der NTP-Daemon auf der vRealize Automation-Appliance stellt synchronisierte Zeitdienste bereit. NTP ist standardmäßig deaktiviert, daher müssen Sie es manuell konfigurieren. Verwenden Sie möglichst NTP in Produktionsumgebungen, um Benutzeraktionen zu verfolgen und potenziell schädliche Angriffe und böswillige Eindringversuche durch akkurate Überwachung und Protokollführung zu erkennen. Informationen zu NTP-Sicherheitshinweisen finden Sie auf der NTP-Website.

Die NTP-Konfigurationsdatei befindet sich im Ordner `/etc/` auf jeder Appliance. Sie können den NTP-Dienst für die vRealize Automation-Appliance aktivieren und Zeitserver auf der Registerkarte **Admin** der Verwaltungsschnittstelle der virtuellen Appliance hinzufügen.

Verfahren

- 1 Öffnen Sie die Konfigurationsdatei `/etc/ntp.conf` auf der Hostmaschine der virtuellen Appliance in einem Texteditor.
- 2 Setzen Sie den Dateibesitzer auf **root:root**.
- 3 Setzen Sie die Berechtigungen auf **0640**.
- 4 Um das Risiko für einen Denial-of-Service-Verstärkungsangriff auf den NTP-Dienst zu verringern, öffnen Sie die Datei `/etc/ntp.conf` und vergewissern Sie sich, dass die eingeschränkten Zeilen in der Datei angezeigt werden.

```
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 die Änderungen und schließen Sie die Dateien.

Konfigurieren von TLS für übertragene Daten der vRealize Automation-Appliance

Stellen Sie sicher, dass Ihre vRealize Automation-Bereitstellung starke TLS-Protokolle verwendet, um Übertragungskkanäle für Komponenten der vRealize Automation-Appliance zu sichern.

Aus Leistungsgründen ist TLS für Localhost-Verbindungen zwischen einigen Anwendungsdiensten nicht aktiviert. In Fällen, bei denen ein umfassender Schutz von Bedeutung ist, aktivieren Sie TLS für alle localhost-Kommunikationen.

Wichtig Wenn Sie TLS auf dem Lastausgleichsdienst beenden, deaktivieren Sie unsichere Protokolle wie SSLv2, SSLv3 und TLS 1.0 auf allen Lastausgleichsdiensten.

Aktivieren von TLS für die Localhost-Konfiguration

Für einige Localhost-Kommunikationen wird TLS standardmäßig nicht verwendet. Sie können TLS über alle Localhost-Verbindungen zur Erhöhung der Sicherheit aktivieren.

Verfahren

- 1 Stellen Sie eine Verbindung mit vRealize Automation-Appliance mithilfe von SSH her.
- 2 Legen Sie Berechtigungen für den vcac-Keystore fest, indem Sie die folgenden Befehle ausführen.

```
usermod -A vco,coredump,pivotal vco
chown vcac.pivotal /etc/vcac/vcac.keystore
chmod 640 /etc/vcac/vcac.keystore
```

- 3 Aktualisieren Sie die HAProxy-Konfiguration.
 - a Öffnen Sie die HAProxy-Konfigurationsdatei unter `/etc/haproxy/conf.d` und wählen Sie den Dienst `20-vcac.cfg` aus.

- b Suchen Sie die Zeilen mit der folgenden Zeichenfolge:

```
server local 127.0.0.1... und fügen Sie Folgendes zum Ende von solchen Zeilen hinzu: ssl
verify none
```

Dieser Abschnitt enthält andere Zeilen ähnlich der folgenden:

backend-horizon	backend-vro
backend-vra	backend-artifactory
backend-vra-health	

- c Ändern Sie den Port für „backend-horizon“ von 8080 in 8443.
- 4 Rufen Sie das Kennwort von keystorePass ab.
 - a Suchen Sie die Eigenschaft `certificate.store.password` in der Datei `/etc/vcac/security.properties`.

Beispielsweise `certificate.store.password=s2enc~iom0GXATG+RB8ff7Wdm4Bg==`

- b Entschlüsseln Sie den Wert mit dem folgenden Befehl:

```
vcac-config prop-util -d --p VALUE
```

Beispielsweise `vcac-config prop-util -d --p s2enc~iom0GXATG+RB8ff7Wdm4Bg==`

5 Konfigurieren Sie den Dienst vRealize Automation.

- a Öffnen Sie die Datei `/etc/vcac/server.xml`.
- b Fügen Sie das folgende Attribut des Konnektor-Tags hinzu und ersetzen Sie „certificate.store.password“ durch den Wert für das Zertifikatspeicherkennwort in `etc/vcac/security.properties`.

```
scheme="https" secure="true" SSLEnabled="true" sslProtocol="TLS" keystoreFile="/etc/vcac/vcac.keystore" keyAlias="apache" keystorePass="certificate.store.password"
```

6 Konfigurieren Sie den vRealize Orchestrator-Dienst.

- a Öffnen Sie die Datei `/etc/vco/app-server.xml`
- b Fügen Sie das folgende Attribut des Konnektor-Tags hinzu und ersetzen Sie „certificate.store.password“ durch den Wert für das Zertifikatspeicherkennwort in `etc/vcac/security.properties`.

```
scheme="https" secure="true" SSLEnabled="true" sslProtocol="TLS" keystoreFile="/etc/vcac/vcac.keystore" keyAlias="apache" keystorePass="certificate.store.password"
```

7 Starten Sie die Dienste vRealize Orchestrator, vRealize Automation und haproxy neu.

```
service vcac-server restart
service vco-server restart
service haproxy restart
```

Hinweis Wenn der vco-server nicht neu gestartet wird, starten Sie den Host-Computer neu.

8 Konfigurieren Sie die Verwaltungsschnittstelle für virtuelle Appliances (Virtual Appliance Management Interface, VAMI).

Sie können den Status der Dienste auflisten, indem Sie den folgenden Befehl auf der virtuellen vRealize Automation-Appliance ausführen.

```
curl -ks -H "Content-Type: application/json" https://localhost/component-registry/services/status/current?limit=200 | jq -re '.content[]|"\(.serviceStatus.serviceName) \(.serviceStatus.serviceInitializationStatus)'"
```

Hinweis Wenn Sie SSL auf der Verwaltungsschnittstelle der virtuellen Appliance aktivieren, kann der Status der vRealize Automation-Dienste nicht auf der Registerkarte „Dienste“ aufgelistet werden.

- a Öffnen Sie die Datei `/opt/vmware/share/htdocs/service/café-services/services.py`.
- b Ändern Sie die Zeile `conn = httpLib.HTTP()` in `conn = httpLib.HTTPS()` zur Erhöhung der Sicherheit.

Aktivieren der Übereinstimmung mit Federal Information Processing Standard (FIPS) 140-2

Die vRealize Automation-Appliance verwendet jetzt die mit dem Federal Information Processing Standard (FIPS) 140-2 zertifizierte Version der OpenSSL-Bibliothek für die Datenübertragung über TLS für den gesamten eingehenden und ausgehenden Netzwerkdatenverkehr.

Sie können den FIPS-Modus in der Verwaltungsschnittstelle der vRealize Automation-Appliance aktivieren oder deaktivieren. Mit den folgenden Befehlen können Sie FIPS auch über die Befehlszeile konfigurieren, während Sie als Root-Benutzer angemeldet sind:

```
vcac-vami fips enable
vcac-vami fips disable
vcac-vami fips status
```

Bei Aktivierung von FIPS verwendet der eingehende und ausgehende Netzwerkdatenverkehr der vRealize Automation-Appliance an Port 443 eine FIPS 140–2-konforme Verschlüsselung. Unabhängig von der FIPS-Einstellung verwendet vRealize Automation AES–256, um gesicherte Daten zu schützen, die auf der vRealize Automation-Appliance gespeichert sind.

Hinweis Die FIPS-Übereinstimmung wird von vRealize Automation derzeit nur teilweise aktiviert, da einige interne Komponenten noch keine zertifizierten Verschlüsselungsmodule verwenden. In Fällen, in denen noch keine zertifizierten Module implementiert wurden, wird die AES-256-basierte Verschlüsselung in allen kryptografischen Algorithmen verwendet.

Hinweis Mithilfe des folgenden Verfahrens können Sie die physische Maschine neu starten, wenn Sie die Konfiguration ändern möchten.

Verfahren

- 1 Melden Sie sich bei der Verwaltungsschnittstelle der vRealize Automation-Appliance als Root-Benutzer an.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Wählen Sie **vRA > Hosteinstellungen** aus.
- 3 Klicken Sie oben rechts auf die Schaltfläche unter der Überschrift „Aktionen“, um FIPS zu aktivieren oder zu deaktivieren.
- 4 Klicken Sie auf **Ja**, um die vRealize Automation-Appliance neu zu starten.

Sicherstellen der Deaktivierung von SSLv3, TLS 1.0 und TLS 1.1

Stellen Sie im Rahmen der Härtung sicher, dass die bereitgestellte vRealize Automation-Appliance sichere Übertragungskanäle verwendet.

Hinweis Nach dem Deaktivieren von TLS 1.0/1.1 und dem Aktivieren von TLS 1.2 können Sie den Vorgang zum Beitreten zum Cluster nicht mehr ausführen.

Voraussetzungen

Führen Sie [Aktivieren von TLS für die Localhost-Konfiguration](#) durch.

Verfahren

- 1 Stellen Sie die Deaktivierung von SSLv3, TLS 1.0 und TLS 1.1 in den HAProxy-HTTP-Handlern auf der vRealize Automation-Appliance sicher.

Überprüfen Sie diese Datei	Stellen Sie sicher, dass folgender Inhalt	in der entsprechenden Zeile wie dargestellt vorhanden ist
/etc/haproxy/conf.d/20-vcac.cfg	no-ssl3 no-tls10 no-tls11 force-tls12	bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-ssl3 no-tls10 no-tls11
/etc/haproxy/conf.d/30-vro-config.cfg	no-ssl3 no-tls10 no-tls11 force-tls12	bind :::8283 v4v6 ssl crt /opt/vmware/etc/lighttpd/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-ssl3 no-tls10 no-tls11

- 2 Starten Sie den Dienst neu.

```
service haproxy restart
```

- 3 Öffnen Sie die Datei /opt/vmware/etc/lighttpd/lighttpd.conf und stellen Sie sicher, dass die richtigen deaktivierten Einträge angezeigt werden.

Hinweis Es gibt keine Direktive zur Deaktivierung von TLS 1.0 oder TLS 1.1 in Lighttpd. Die Beschränkung für die Verwendung von TLS 1.0 und TLS 1.1 kann teilweise abgeschwächt werden, indem erzwungen wird, dass OpenSSL keine Verschlüsselungen von TLS 1.0 und TLS 1.1 verwendet.

```
ssl.use-ssl2 = "disable"
ssl.use-ssl3 = "disable"
```

- 4 Stellen Sie die Deaktivierung von SSLv3, TLS 1.0 und TLS 1.1 für den Konsolenproxy auf der vRealize Automation-Appliance sicher.
 - a Bearbeiten Sie die Datei /etc/vcac/security.properties, indem Sie die folgende Zeile hinzufügen oder ändern:


```
consoleproxy.ssl.server.protocols = TLSv1.2
```
 - b Starten Sie den Server neu, indem Sie den folgenden Befehl ausführen:


```
service vcac-server restart
```

- 5** Vergewissern Sie sich, dass SSLv3, TLS 1.0 und TLS 1.1 für den vCO-Dienst deaktiviert ist.
- a Suchen Sie das Tag <Connector> in der Datei /etc/vco/app-server/server.xml und fügen Sie das folgende Attribut hinzu:

```
sslEnabledProtocols = "TLSv1.2"
```

- b Starten Sie den vCO-Dienst neu, indem Sie den folgenden Befehl ausführen.

```
service vco-server restart
```

- 6** Vergewissern Sie sich, dass SSLv3, TLS 1.0 und TLS 1.1 für den vRealize Automation-Dienst deaktiviert ist.

- a Fügen Sie die folgenden Attribute zum Tag <Connector> in der Datei /etc/vcac/server.xml hinzu.

```
sslEnabledProtocols = "TLSv1.2"
```

- b Starten Sie den vRealize Automation-Dienst neu, indem Sie den folgenden Befehl ausführen:

```
service vcac-server restart
```

- 7** Vergewissern Sie sich, dass SSLv3, TLS 1.0 und TLS 1.1 für RabbitMQ deaktiviert ist.

Öffnen Sie die Datei /etc/rabbitmq/rabbitmq.config und stellen Sie sicher, dass nur {versions, ['tlsv1.2']} in den Abschnitten „ssl“ und „ssl_options“ vorhanden ist.

```
[
  {ssl, [
    {versions, ['tlsv1.2']},
    {ciphers, ["AES256-SHA", "AES128-SHA"]}
  ]},
  {rabbit, [
    {tcp_listeners, [{"127.0.0.1", 5672}]},
    {frame_max, 262144},
    {ssl_listeners, [5671]},
    {ssl_options, [
      {cacertfile, "/etc/rabbitmq/certs/ca/cacert.pem"},
      {certfile, "/etc/rabbitmq/certs/server/cert.pem"},
      {keyfile, "/etc/rabbitmq/certs/server/key.pem"},
      {versions, ['tlsv1.2']},
      {ciphers, ["AES256-SHA", "AES128-SHA"]},
      {verify, verify_peer},
      {fail_if_no_peer_cert, false}
    ]},
    {mnesia_table_loading_timeout, 600000},
    {cluster_partition_handling, autoheal},
    {heartbeat, 600}
  ]},
  {kernel, [{net_ticktime, 120}]}
].
```

- 8** Starten Sie den RabbitMQ-Server neu.

```
# service rabbitmq-server restart
```

- 9 Vergewissern Sie sich, dass SSLv3, TLS 1.0 und TLS 1.1 für den vIDM-Dienst deaktiviert ist.

Öffnen Sie die Datei `opt/vmware/horizon/workspace/conf/server.xml` für jede Konnektorinstanz, die `SSLEnabled="true"` enthält, und stellen Sie sicher, dass die folgende Zeile vorhanden ist.

```
sslEnabledProtocols="TLSv1.2"
```

Konfigurieren von TLS-Verschlüsselungs-Suites für vRealize Automation-Komponenten

Für maximale Sicherheit müssen Sie vRealize Automation-Komponenten für die Verwendung starker Verschlüsselungen konfigurieren.

Die zwischen dem Server und dem Browser ausgehandelte Verschlüsselungsschiffre bestimmt die Verschlüsselungsstärke, die in einer TLS-Sitzung verwendet wird.

Um sicherzustellen, dass nur starke Verschlüsselungen ausgewählt werden, deaktivieren Sie schwache Verschlüsselungen in vRealize Automation-Komponenten. Konfigurieren Sie den Server so, dass er nur starke Verschlüsselungen unterstützt und ausreichend große Schlüsselgrößen verwendet. Konfigurieren Sie außerdem alle Verschlüsselungen in einer geeigneten Reihenfolge.

Deaktivieren Sie Verschlüsselungs-Suites, die keine Authentifizierung bieten, wie NULL-Verschlüsselungs-Suites, aNULL oder eNULL. Deaktivieren Sie auch anonymen Diffie-Hellman-Schlüsselaustausch (ADH), Export Level Cipher-Instanzen (EXP, Verschlüsselungen, die DES enthalten), Schlüsselgrößen unter 128 Bit für die Verschlüsselung von Nutzlast-Datenverkehr, die Verwendung von MD5 als Hashing-Mechanismus für Nutzlast-Datenverkehr, IDEA-Verschlüsselungs-Suites und RC4-Verschlüsselungs-Suites. Stellen Sie außerdem sicher, dass Verschlüsselungs-Suites, die den Diffie-Hellman (DHE)-Schlüsselaustausch verwenden, deaktiviert sind.

Weitere Informationen zum Deaktivieren von TLS finden Sie im [Knowledge Base-Artikel 2146570](#).

Deaktivieren von schwachen Verschlüsselungen im HA-Proxydienst

Überprüfen Sie die Verschlüsselungen im HA-Proxydienst für die vRealize Automation-Appliance anhand der Liste der zulässigen Verschlüsselungen und deaktivieren Sie alle schwachen Verschlüsselungen.

Deaktivieren Sie Verschlüsselungs-Suites, die keine Authentifizierung bieten, wie NULL-Verschlüsselungs-Suites, aNULL oder eNULL. Deaktivieren Sie auch anonymen Diffie-Hellman-Schlüsselaustausch (ADH), Export Level Cipher-Instanzen (EXP, Verschlüsselungen, die DES enthalten), Schlüsselgrößen unter 128 Bit für die Verschlüsselung von Nutzlast-Datenverkehr, die Verwendung von MD5 als Hashing-Mechanismus für Nutzlast-Datenverkehr, IDEA-Verschlüsselungs-Suites und RC4-Verschlüsselungs-Suites.

Verfahren

- 1 Überprüfen Sie die Verschlüsselungseintrag der Bind-Direktive in der Datei `/etc/haproxy/conf.d/20-vcac.cfg` und deaktivieren Sie alle schwachen Verschlüsselungen.

```
bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-ssl3 no-tls10 no-tls11
```

- Überprüfen Sie die Verschlüsselungseintrag der Bind-Direktive in der Datei `/etc/haproxy/conf.d/30-vro-config.cfg` und deaktivieren Sie alle schwachen Verschlüsselungen.

```
bind :::8283 v4v6 ssl crt /opt/vmware/etc/lighttpd/server.pem ciphers !aNULL:!eNULL:kECDH
+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-ssl3 no-tls10 no-
tls11
```

Deaktivieren von schwachen Verschlüsselungen im vRealize Automation-Appliance-Konsolenproxydienst der vRealize Automation-Appliance

Überprüfen Sie die Verschlüsselungen im Konsolenproxydienst der vRealize Automation-Appliance anhand der Liste der zulässigen Verschlüsselungen und deaktivieren Sie alle schwachen Verschlüsselungen.

Deaktivieren Sie Verschlüsselungs-Suites, die keine Authentifizierung bieten, wie NULL-Verschlüsselungs-Suites, aNULL oder eNULL. Deaktivieren Sie auch anonymen Diffie-Hellman-Schlüsselaustausch (ADH), Export Level Cipher-Instanzen (EXP, Verschlüsselungen, die DES enthalten), Schlüsselgrößen unter 128 Bit für die Verschlüsselung von Nutzlast-Datenverkehr, die Verwendung von MD5 als Hashing-Mechanismus für Nutzlast-Datenverkehr, IDEA-Verschlüsselungs-Suites und RC4-Verschlüsselungs-Suites.

Verfahren

- Öffnen Sie die Datei `/etc/vcac/security.properties` in einem Texteditor.
- Fügen Sie eine Zeile zur Datei hinzu, um die unerwünschten Verschlüsselungen zu deaktivieren.

Verwenden Sie eine Variante der folgenden Zeile:

```
consoleproxy.ssl.ciphers.disallowed=cipher_suite_1, cipher_suite_2 usw.
```

Um zum Beispiel die AES 128- und AES 256-Verschlüsselungen zu deaktivieren, fügen Sie die folgende Zeile hinzu:

```
consoleproxy.ssl.ciphers.disallowed=TLS_DH_DSS_WITH_AES_128_CBC_SHA,
TLS_DH_DSS_WITH_AES_256_CBC_SHA, TLS_DH_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

- Starten Sie den Server mit nachfolgend aufgeführtem Befehl neu.

```
service vcac-server restart
```

Deaktivieren von schwachen Verschlüsselungen im vRealize Automation-Appliance-vCO-Dienst

Überprüfen Sie die Verschlüsselungen im vRealize Automation-Appliance-vCO-Dienst anhand der Liste der zulässigen Verschlüsselungen und deaktivieren Sie alle schwachen Verschlüsselungen.

Deaktivieren Sie Verschlüsselungs-Suites, die keine Authentifizierung bieten, wie NULL-Verschlüsselungs-Suites, aNULL oder eNULL. Deaktivieren Sie auch anonymen Diffie-Hellman-Schlüsselaustausch (ADH), Export Level Cipher-Instanzen (EXP, Verschlüsselungen, die DES enthalten), Schlüsselgrößen unter 128 Bit für die Verschlüsselung von Nutzlast-Datenverkehr, die Verwendung von MD5 als Hashing-Mechanismus für Nutzlast-Datenverkehr, IDEA-Verschlüsselungs-Suites und RC4-Verschlüsselungs-Suites.

Verfahren

- 1 Suchen Sie das Tag <Connector> in der Datei /etc/vco/app-server/server.xml.
- 2 Bearbeiten oder fügen Sie das Verschlüsselungsattribut hinzu, um die gewünschten Verschlüsselungs-Suites zu verwenden.

Informationen hierzu finden Sie im folgenden Beispiel:

```
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
```

Deaktivieren von schwachen Verschlüsselungen im vRealize Automation-Appliance-RabbitMQ-Dienst

Überprüfen Sie die Verschlüsselungen im vRealize Automation-Appliance-RabbitMQ-Dienst anhand der Liste der zulässigen Verschlüsselungen und deaktivieren Sie alle schwachen Verschlüsselungen.

Deaktivieren Sie Verschlüsselungs-Suites, die keine Authentifizierung bieten, wie NULL-Verschlüsselungs-Suites, aNULL oder eNULL. Deaktivieren Sie auch anonymen Diffie-Hellman-Schlüsselaustausch (ADH), Export Level Cipher-Instanzen (EXP, Verschlüsselungen, die DES enthalten), Schlüsselgrößen unter 128 Bit für die Verschlüsselung von Nutzlast-Datenverkehr, die Verwendung von MD5 als Hashing-Mechanismus für Nutzlast-Datenverkehr, IDEA-Verschlüsselungs-Suites und RC4-Verschlüsselungs-Suites.

Verfahren

- 1 Überprüfen Sie die unterstützten Verschlüsselungs-Suites, indem Sie den Befehl # /usr/sbin/rabbitmqctl eval 'ssl:cipher_suites().' ausführen.

Die im folgenden Beispiel zurückgegebenen Verschlüsselungen stellen nur die unterstützten Verschlüsselungen dar. Der RabbitMQ-Server verwendet diese Verschlüsselungen nicht bzw. kündigt diese nicht an, es sei denn, diese Vorgehensweise ist in der Datei rabbitmq.config konfiguriert.

```
["ECDHE-ECDSA-AES256-GCM-SHA384", "ECDHE-RSA-AES256-GCM-SHA384",
 "ECDHE-ECDSA-AES256-SHA384", "ECDHE-RSA-AES256-SHA384",
 "ECDH-ECDSA-AES256-GCM-SHA384", "ECDH-RSA-AES256-GCM-SHA384",
 "ECDH-ECDSA-AES256-SHA384", "ECDH-RSA-AES256-SHA384",
 "DHE-RSA-AES256-GCM-SHA384", "DHE-DSS-AES256-GCM-SHA384",
 "DHE-RSA-AES256-SHA256", "DHE-DSS-AES256-SHA256", "AES256-GCM-SHA384",
 "AES256-SHA256", "ECDHE-ECDSA-AES128-GCM-SHA256",
 "ECDHE-RSA-AES128-GCM-SHA256", "ECDHE-ECDSA-AES128-SHA256",
 "ECDHE-RSA-AES128-SHA256", "ECDH-ECDSA-AES128-GCM-SHA256",
```

```
"ECDH-RSA-AES128-GCM-SHA256", "ECDH-ECDSA-AES128-SHA256",
"ECDH-RSA-AES128-SHA256", "DHE-RSA-AES128-GCM-SHA256",
"DHE-DSS-AES128-GCM-SHA256", "DHE-RSA-AES128-SHA256", "DHE-DSS-AES128-SHA256",
"AES128-GCM-SHA256", "AES128-SHA256", "ECDHE-ECDSA-AES256-SHA",
"ECDHE-RSA-AES256-SHA", "DHE-RSA-AES256-SHA", "DHE-DSS-AES256-SHA",
"ECDH-ECDSA-AES256-SHA", "ECDH-RSA-AES256-SHA", "AES256-SHA",
"ECDHE-ECDSA-DES-CBC3-SHA", "ECDHE-RSA-DES-CBC3-SHA", "EDH-RSA-DES-CBC3-SHA",
"EDH-DSS-DES-CBC3-SHA", "ECDH-ECDSA-DES-CBC3-SHA", "ECDH-RSA-DES-CBC3-SHA",
"DES-CBC3-SHA", "ECDHE-ECDSA-AES128-SHA", "ECDHE-RSA-AES128-SHA",
"DHE-RSA-AES128-SHA", "DHE-DSS-AES128-SHA", "ECDH-ECDSA-AES128-SHA",
"ECDH-RSA-AES128-SHA", "AES128-SHA"]
```

- 2 Wählen Sie die unterstützten Verschlüsselungen aus, die den Sicherheitsanforderungen Ihrer Organisation entsprechen.

Um beispielsweise nur ECDHE-ECDSA-AES128-GCM-SHA256 & ECDHE-ECDSA-AES256-GCM-SHA384 zuzulassen, überprüfen Sie die Datei `/etc/rabbitmq/rabbitmq.config` und fügen Sie die folgende Zeile unter „`ssl`“ und „`ssl_options`“ hinzu.

```
{ciphers, ["ECDHE-ECDSA-AES128-GCM-SHA256", "ECDHE-ECDSA-AES256-GCM-SHA384"]}
```

- 3 Starten Sie den RabbitMQ-Server mithilfe des folgenden Befehls neu.

```
service rabbitmq-server restart
```

Überprüfen der Sicherheit von Data-at-Rest

Überprüfen Sie die Sicherheit der mit vRealize Automation verwendeten Datenbankbenutzer und -konten.

Postgres-Benutzer

Das Postgres-Linux-Benutzerkonto ist mit der Rolle des Postgres-Datenbankadministrators verknüpft und ist standardmäßig ein gesperrtes Konto. Dies ist die sicherste Konfiguration für diesen Benutzer, da der Zugriff nur über das Root-Benutzerkonto erfolgen kann. Entsperren Sie dieses Konto nicht.

Rollen für Datenbankbenutzerkonten

Die Standardrollen für Postgres-Benutzerkonten sollten nicht für Funktionen verwendet werden, bei denen es sich nicht um Anwendungsfunktionen handelt. Zur Unterstützung von nicht standardmäßigen Aktivitäten zur Datenbanküberprüfung und zur Erstellung von Datenbankberichten sollte ein zusätzliches Konto mit einem entsprechend geschützten Kennwort erstellt werden.

Führen Sie in der Befehlszeile das folgende Skript aus:

```
vcac-vami add-db-user newUsername newPassword
```

Hiermit wird ein neuer Benutzer und ein vom Benutzer angegebenes Kennwort hinzugefügt.

Hinweis Dieses Skript muss in den Fällen für die Master-Postgres-Datenbank ausgeführt werden, in denen ein Master-Slave-HA-Postgres-Setup konfiguriert ist.

Konfigurieren der PostgreSQL-Clientauthentifizierung

Stellen Sie sicher, dass die Authentifizierung der lokalen Vertrauensstellung nicht für die PostgreSQL-Datenbank der vRealize Automation-Appliance konfiguriert ist. Diese Konfiguration ermöglicht jedem lokalen Benutzer, einschließlich des Datenbankadministrators, ohne Kennwort eine Verbindung als PostgreSQL-Benutzer herzustellen.

Hinweis Für das Postgres-Superuser-Konto sollte eine lokale Vertrauensstellung beibehalten werden.

Die md5-Authentifizierungsmethode wird empfohlen, da sie verschlüsselte Kennwörter sendet.

Die Konfigurationseinstellungen der Clientauthentifizierung befinden sich in der Datei `/storage/db/pgdata/pg_hba.conf`.

#	TYPE	DATABASE	USER	ADDRESS	METHOD
# "local" is for Unix domain socket connections only					
local	all		postgres		trust
# IPv4 local connections:					
#host	all		all	127.0.0.1/32	md5
hostssl	all		all	127.0.0.1/32	md5
# IPv6 local connections:					
#host	all		all	:::1/128	md5
hostssl	all		all	:::1/128	md5
# Allow remote connections for VCAC user.					
#host	vcac		vcac	0.0.0.0/0	md5
hostssl	vcac		vcac	0.0.0.0/0	md5
hostssl	vcac		vcac	:::0/0	md5
# Allow remote connections for VCAC replication user.					
#host	vcac		vcac_replication	0.0.0.0/0	md5
hostssl	vcac		vcac_replication	0.0.0.0/0	md5
hostssl	vcac		vcac_replication	:::0/0	md5
# Allow replication connections by a user with the replication privilege.					
#host	replication		vcac_replication	0.0.0.0/0	md5
hostssl	replication		vcac_replication	0.0.0.0/0	md5
hostssl	replication		vcac_replication	:::0/0	md5

Wenn Sie die Datei `pg_hba.conf` bearbeiten, müssen Sie den Postgres-Server neu starten, indem Sie die folgenden Befehle ausführen, bevor die Änderungen wirksam werden können.

```
# cd /opt/vmware/vpostgres/9.2/bin
# su postgres
# ./pg_ctl restart -D /storage/db/pgdata/ -m fast
```

Konfigurieren von vRealize Automation-Anwendungsressourcen

Überprüfen Sie die vRealize Automation-Anwendungsressourcen und beschränken Sie die Dateiberechtigungen.

Verfahren

- 1 Führen Sie den folgenden Befehl aus, um sicherzustellen, dass Dateien mit SUID- und GUID-Bits ordnungsgemäß definiert sind.

```
find / -path /proc -prune -o -type f -perm +6000 -ls
```

Die folgende Liste wird angezeigt.

```
2197357  24 -rwsr-xr-x  1 polkituser root      23176 Mar 31  2015 /usr/lib/PolicyKit/polkit-
set-default-helper
2197354  16 -rwxr-sr-x  1 root      polkituser  14856 Mar 31  2015 /usr/lib/PolicyKit/polkit-
read-auth-helper
2197353  12 -rwsr-x---  1 root      polkituser  10744 Mar 31  2015 /usr/lib/PolicyKit/polkit-
grant-helper-pam
2197352  20 -rwxr-sr-x  1 root      polkituser  19208 Mar 31  2015 /usr/lib/PolicyKit/polkit-
grant-helper
2197351  20 -rwxr-sr-x  1 root      polkituser  19008 Mar 31  2015 /usr/lib/PolicyKit/polkit-
explicit-grant-helper
2197356  24 -rwxr-sr-x  1 root      polkituser  23160 Mar 31  2015 /usr/lib/PolicyKit/polkit-
revoke-helper
2188203  460 -rws--x--x  1 root      root      465364 Apr 21 22:38 /usr/lib64/ssh/ssh-keysign
2138858  12 -rwxr-sr-x  1 root      tty       10680 May 10  2010 /usr/sbin/utempter
2142482  144 -rwsr-xr-x  1 root      root      142890 Sep 15  2015 /usr/bin/passwd
2142477  164 -rwsr-xr-x  1 root      shadow    161782 Sep 15  2015 /usr/bin/chage
2142467  156 -rwsr-xr-x  1 root      shadow    152850 Sep 15  2015 /usr/bin/chfn
1458298  364 -rwsr-xr-x  1 root      root      365787 Jul 22  2015 /usr/bin/sudo
2142481  64 -rwsr-xr-x  1 root      root      57776 Sep 15  2015 /usr/bin/newgrp
1458249  40 -rwsr-x---  1 root      trusted   40432 Mar 18  2015 /usr/bin/crontab
2142478  148 -rwsr-xr-x  1 root      shadow    146459 Sep 15  2015 /usr/bin/chsh
2142480  156 -rwsr-xr-x  1 root      shadow    152387 Sep 15  2015 /usr/bin/gpasswd
2142479  48 -rwsr-xr-x  1 root      shadow    46967 Sep 15  2015 /usr/bin/expiry
311484  48 -rwsr-x---  1 root      messagebus 47912 Sep 16  2014 /lib64/dbus-1/dbus-daemon-
launch-helper
876574  36 -rwsr-xr-x  1 root      shadow    35688 Apr 10  2014 /sbin/unix_chkpwd
876648  12 -rwsr-xr-x  1 root      shadow    10736 Dec 16  2011 /sbin/unix2_chkpwd
 49308  68 -rwsr-xr-x  1 root      root      63376 May 27  2015 /opt/likewise/bin/ksu
1130552  40 -rwsr-xr-x  1 root      root      40016 Apr 16  2015 /bin/su
1130511  40 -rwsr-xr-x  1 root      root      40048 Apr 15  2011 /bin/ping
1130600  100 -rwsr-xr-x  1 root      root      94808 Mar 11  2015 /bin/mount
1130601  72 -rwsr-xr-x  1 root      root      69240 Mar 11  2015 /bin/umount
1130512  36 -rwsr-xr-x  1 root      root      35792 Apr 15  2011 /bin/ping6  2012 /lib64/
dbus-1/dbus-daemon-launch-helper
```

- 2 Führen Sie den folgenden Befehl aus, um sicherzustellen, dass alle Dateien auf der virtuellen Appliance einen Besitzer haben.

```
find / -path /proc -prune -o -nouser -o -nogroup
```

- 3 Überprüfen Sie die Berechtigungen für alle Dateien auf der virtuellen Appliance, um sicherzustellen, dass keine von jedermann beschreibbar ist, indem Sie den folgenden Befehl ausführen.

```
find / -name "*.*" -type f -perm -a+w | xargs ls -ldb
```

- 4 Führen Sie den folgenden Befehl aus, um sicherzustellen, dass nur der vCAC-Benutzer die richtigen Dateien besitzt.

```
find / -name "proc" -prune -o -user vcac -print | egrep -v -e "*/vcac/*" | egrep -v -e "*/vmware-vcac/*"
```

Wenn keine Ergebnisse angezeigt werden, gehören alle Dateien nur dem vCAC-Benutzer.

- 5 Stellen Sie sicher, dass nur der vCAC-Benutzer Schreibrechte für die folgenden Dateien besitzt.

```
/etc/vcac/vcac/security.properties
/etc/vcac/vcac/solution-users.properties
/etc/vcac/vcac/sso-admin.properties
/etc/vcac/vcac/vcac.keystore
/etc/vcac/vcac/vcac.properties
```

Überprüfen Sie außerdem die folgenden Dateien und deren Unterverzeichnisse:

```
/var/log/vcac/*
/var/lib/vcac/*
/var/cache/vcac/*
```

- 6 Stellen Sie sicher, dass die richtigen Dateien in den folgenden Verzeichnissen und Unterverzeichnissen nur vom vCAC- oder Root-Benutzer gelesen werden können.

```
/etc/vcac/*
/var/log/vcac/*
/var/lib/vcac/*
/var/cache/vcac/*
```

- 7 Stellen Sie sicher, dass die richtigen Dateien nur im Besitz des vCO- oder Root-Benutzers sind, wie in den folgenden Verzeichnissen und deren Unterverzeichnissen dargestellt.

```
/etc/vco/*
/var/log/vco/*
/var/lib/vco/*
/var/cache/vco/*
```

- 8 Stellen Sie sicher, dass die richtigen Dateien nur vom vCO- oder Root-Benutzer beschrieben werden können, wie in den folgenden Verzeichnissen und Unterverzeichnissen dargestellt.

```
/etc/vco/*
/var/log/vco/*
/var/lib/vco/*
/var/cache/vco/*
```

- 9 Stellen Sie sicher, dass die richtigen Dateien nur vom vCO- oder Root-Benutzer gelesen werden können, wie in den folgenden Verzeichnissen und Unterverzeichnissen dargestellt.

```
/etc/vco/*
/var/log/vco/*
/var/lib/vco/*
/var/cache/vco/*
```

Anpassen der Konsolen-Proxykonfiguration

Sie können die Remote-Konsolenkonfiguration für vRealize Automation zur Erleichterung der Fehlerbehebung und organisatorischen Vorgehensweisen anpassen.

Wenn Sie vRealize Automation installieren, konfigurieren oder verwalten, können Sie einige Einstellungen ändern, um Fehlerbehebung und Debugging Ihrer Installation zu aktivieren. Katalogisieren und prüfen Sie alle vorgenommenen Änderungen, um sicherzustellen, dass anwendbare Komponenten entsprechend ihrer erforderlichen Verwendung korrekt abgesichert sind. Fahren Sie erst dann mit der Produktion fort, wenn Sie sicher sind, dass die Änderungen der Konfiguration korrekt abgesichert sind.

Anpassen des VMware Remote Console-Ticketablaufs

Sie können die Gültigkeitsdauer für Remote-Konsolen-Tickets, die für das Herstellen von VMware Remote Console-Verbindungen verwendet werden, anpassen.

Wenn ein Benutzer VMware Remote Console-Verbindungen herstellt, gibt das System neu erstellte, einmalige Anmeldedaten zurück, die eine bestimmte Verbindung zu einer virtuellen Maschine herstellen. Sie können den Ticketablauf für einen angegebenen Zeitraum in Minuten festlegen.

Verfahren

- 1 Öffnen Sie die Datei `/etc/vcac/security.properties` in einem Texteditor.
- 2 Fügen Sie in der Datei eine Zeile im Format `consoleproxy.ticket.validitySec=30` hinzu.
Der numerische Wert in dieser Zeile gibt die Anzahl der Minuten an, bis das Ticket abläuft.
- 3 Speichern Sie die Datei und schließen Sie sie.
- 4 Starten Sie den vCAC-Server unter Verwendung des Befehls `/etc/init.d/vcac-server restart` neu.
Der Wert für den Ticketablauf wird auf den angegebenen Zeitraum in Minuten zurückgesetzt.

Anpassen des Konsolen-Proxyserver-Ports

Sie können den Port anpassen, auf dem der VMware Remote Console-Konsolenproxy Nachrichten empfängt.

Verfahren

- 1 Öffnen Sie die Datei `/etc/vcac/security.properties` in einem Texteditor.

- 2 Fügen Sie in der Datei eine Zeile im Format `consoleproxy.service.port=8445` hinzu.

Der numerische Wert gibt die Nummer des Konsolen-Proxydienst-Ports an, die in diesem Fall 8445 ist.

- 3 Speichern Sie die Datei und schließen Sie sie.
- 4 Starten Sie den vCAC-Server unter Verwendung des Befehls `/etc/init.d/vcac-server restart` neu.
Der Proxydienst-Port wird in die angegebene Portnummer geändert.

Konfigurieren der X-XSS-Schutz-Antwortkopfzeile

Fügen Sie die X-XSS-Schutz-Antwortkopfzeile der haproxy-Konfigurationsdatei hinzu.

Verfahren

- 1 Öffnen Sie `/etc/haproxy/conf.d/20-vcac.cfg` zur Bearbeitung.
- 2 Fügen Sie die folgenden Zeilen in einem Front-End-Abschnitt hinzu:

```
rspdel X-XSS-Protection:\ 1;\ mode=block
rspadd X-XSS-Protection:\ 1;\ mode=block
```

- 3 Laden Sie die HAProxy-Konfiguration mithilfe des folgenden Befehls neu.
`/etc/init.d/haproxy reload`

Konfigurieren des Antwortheaders „X-Content-Type-Options“

Fügen Sie den Antwortheader „X-Content-Type-Options“ zur HAProxy-Konfiguration hinzu.

Verfahren

- 1 Öffnen Sie `/etc/haproxy/conf.d/20-vcac.cfg` zur Bearbeitung.
- 2 Fügen Sie die folgenden Zeilen in einem Front-End-Abschnitt hinzu:

```
http-response set-header X-Content-Type-Options nosniff
```

- 3 Laden Sie die HAProxy-Konfiguration mithilfe des folgenden Befehls neu.
`/etc/init.d/haproxy reload`

Konfigurieren der HTTP Strict Transport Security-Antwortkopfzeile

Fügen Sie die HTTP Strict Transport Security(HSTS)-Antwortkopfzeile der HAProxy-Konfiguration hinzu.

Verfahren

- 1 Öffnen Sie `/etc/haproxy/conf.d/20-vcac.cfg` zur Bearbeitung.

- 2 Fügen Sie die folgenden Zeilen in einem Front-End-Abschnitt hinzu:

```
rspdel Strict-Transport-Security:\ max-age=31536000
rspadd Strict-Transport-Security:\ max-age=31536000
```

- 3 Laden Sie die HAProxy-Konfiguration mithilfe des folgenden Befehls neu.

```
/etc/init.d/haproxy reload
```

Konfigurieren der X-Frame-Options-Antwortkopfzeile

Die X-Frame-Options-Antwortkopfzeile wird möglicherweise in einigen Fällen zweimal angezeigt.

Die X-Frame-Options-Antwortkopfzeile wird möglicherweise zweimal angezeigt, da der vIDM-Dienst diese Kopfzeile dem Back-End sowie HAProxy hinzufügt. Sie können mit einer entsprechenden Konfiguration verhindern, dass er zweimal angezeigt wird.

Verfahren

- 1 Öffnen Sie `/etc/haproxy/conf.d/20-vcac.cfg` zur Bearbeitung.

- 2 Suchen Sie die folgende Zeile im Front-End-Abschnitt:

```
rspadd X-Frame-Options:\ SAMEORIGIN
```

- 3 Fügen Sie die folgenden Zeilen vor der Zeile ein, die Sie im vorherigen Schritt ermittelt haben:

```
rspdel X-Frame-Options:\ SAMEORIGIN
```

- 4 Laden Sie die HAProxy-Konfiguration mithilfe des folgenden Befehls neu.

```
/etc/init.d/haproxy reload
```

Konfigurieren von Server-Antwortkopfzeilen

Aus Sicherheitsgründen wird die Konfiguration Ihres vRealize Automation-Systems zur Beschränkung der für potenzielle Angreifer verfügbaren Informationen empfohlen.

Minimieren Sie die Menge der Informationen soweit wie möglich, die Ihr System über seine Identität und Version offen legt. Hacker und Kriminelle können diese Informationen für zielgerichtete Angriffe auf Ihren Webserver verwenden.

Konfigurieren der Lighttpd-Server-Antwortkopfzeile

Erstellen Sie als Best Practice eine leere Serverkopfzeile für den lighttpd-Server der vRealize Automation-Appliance.

Verfahren

- 1 Öffnen Sie die Datei `/opt/vmware/etc/lighttpd/lighttpd.conf` in einem Texteditor.
- 2 Fügen Sie `server.tag = " "` der Datei hinzu.
- 3 Speichern Sie die Änderungen und schließen Sie die Datei.

- 4 Starten Sie den `lighttpd`-Server durch Ausführen des Befehls `# /opt/vmware/etc/init.d/vami-lighttpd restart` neu.

Konfigurieren der TCServer-Antwortkopfzeile für die vRealize Automation-Appliance

Erstellen Sie als Best Practice eine benutzerdefinierte leere Serverkopfzeile für die TCServer-Antwortkopfzeile, die mit der vRealize Automation-Appliance verwendet wird, um die Möglichkeit bössartiger Angreifer einzuschränken, an wertvolle Informationen zu gelangen.

Verfahren

- 1 Öffnen Sie die Datei `/etc/vco/app-server/server.xml` in einem Texteditor.
- 2 Hinzufügen von `server=" "` in jedem `<Connector>`-Element
Beispiel: `<Connector protocol="HTTP/1.1" server="" />`
- 3 Speichern Sie die Änderungen und schließen Sie die Datei.
- 4 Starten Sie den Server mit nachfolgend aufgeführtem Befehl neu.

```
service vco-server restart
```

Konfigurieren der Antwortkopfzeile des Internet Information Services-Servers

Erstellen Sie als Best Practice eine benutzerdefinierte leere Serverkopfzeile für den Internet Information Services(IIS)-Server, die mit der Identity Appliance verwendet wird, um die Möglichkeit bössartiger Angreifer einzuschränken, an wertvolle Informationen zu gelangen.

Verfahren

- 1 Öffnen Sie die Datei `C:\Windows\System32\inetsrv\urlscan\UrlScan.ini` in einem Texteditor.
- 2 Suchen Sie nach `RemoveServerHeader=0` und ändern Sie den Ausdruck in `RemoveServerHeader=1..`
- 3 Speichern Sie die Änderungen und schließen Sie die Datei.
- 4 Führen Sie den Befehl `iisreset` aus, um den Server neu zu starten.

Nächste Schritte

Deaktivieren Sie die IIS X-Powered By-Kopfzeile, indem Sie HTTP-Antwortkopfzeilen aus der Liste in der IIS-Manager-Konsole entfernen.

- 1 Öffnen Sie die IIS-Manager-Konsole.
- 2 Öffnen Sie die HTTP-Antwortkopfzeile und entfernen Sie sie aus der Liste.
- 3 Führen Sie den Befehl `iisreset` aus, um den Server neu zu starten.

Festlegen der Zeitüberschreitung für eine vRealize Automation-Appliance-Sitzung

Konfigurieren Sie den Zeitüberschreitungswert für die Sitzung auf der vRealize Automation-Appliance gemäß den Sicherheitsrichtlinien Ihres Unternehmens.

Der standardmäßige Zeitüberschreitungswert bei Inaktivität für eine vRealize Automation-Appliance-Sitzung beträgt 30 Minuten. Um diesen Wert gemäß den Sicherheitsrichtlinien Ihres Unternehmens anzupassen, bearbeiten Sie die Datei `web.xml` auf Ihrer vRealize Automation-Appliance-Hostmaschine.

Verfahren

- 1 Öffnen Sie die Datei `/usr/lib/vcac/server/webapps/vcac/WEB-INF/web.xml` in einem Texteditor.
- 2 Suchen Sie den Eintrag `session-config` und legen Sie den Wert für Zeitüberschreitung der Sitzung fest. Schauen Sie sich das folgende Codebeispiel an.

```
<!-- 30 minutes session expiration time -->
<session-config>
  <session-timeout>30</session-timeout>
  <tracking-mode>COOKIE</tracking-mode>
  <cookie-config>
    <path>/</path>
  </cookie-config>
</session-config>
```

- 3 Starten Sie den Server neu, indem Sie den folgenden Befehl ausführen.

```
service vcac-server restart
```

Verwalten nicht erforderlicher Software

Um Sicherheitsrisiken zu minimieren, entfernen Sie nicht erforderliche Software von Ihren vRealize Automation-Hostmaschinen.

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

Sichern des USB-Massenspeicher-Handlers

Sichern Sie den USB-Massenspeicher-Handler, um dessen Verwendung als USB-Geräte-Handler mit Hostmaschinen der virtuellen VMware-Appliances zu verhindern. Potenzielle Angreifer können diesen Handler ausnutzen, um Ihr System zu gefährden.

Verfahren

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

Sichern des Bluetooth-Protokoll-Handlers

Sichern Sie den Bluetooth-Protokoll-Handler auf den Hostmaschinen Ihrer virtuellen Appliances, um potenzielle Angriffe zu verhindern.

Das Binden des Bluetooth-Protokolls an den Netzwerkstapel ist nicht erforderlich und kann den Host für Angriff anfälliger machen.

Verfahren

- 1 Öffnen Sie die Datei `/etc/modprobe.conf.local` in einem Texteditor.
- 2 Stellen Sie sicher, dass in dieser Datei die folgende Zeile angezeigt wird.

```
install bluetooth /bin/true
```

- 3 Speichern Sie die Datei und schließen Sie sie.

Sichern des SCTP (Stream Control Transmission Protocol)-Protokolls

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

Konfigurieren Sie Ihr System, um zu verhindern, dass das SCTP-Modul geladen wird, sofern dies nicht absolut notwendig ist. SCTP ist ein nicht verwendetes, durch IETF standardisiertes Transportebenenprotokoll. Wenn Sie das AppleTalk-Protokoll an den Netzwerkstapel binden, ist der Host für Angriffe anfälliger. Nicht berechnete lokale Prozesse können dazu führen, dass der Kernel einen Protokoll-Handler dynamisch lädt, indem er ein Socket mit dem Protokoll öffnet.

Verfahren

- 1 Öffnen Sie die Datei `/etc/modprobe.conf.local` in einem Texteditor.
- 2 Stellen Sie sicher, dass in dieser Datei die folgende Zeile angezeigt wird.

```
install sctp /bin/true
```

- 3 Speichern Sie die Datei und schließen Sie sie.

Sichern des DCCP (Datagram Congestion Protocol)-Protokolls

Im Rahmen der Härtung Ihrer Systemaktivitäten sollte das DCCP-Protokoll nicht standardmäßig auf den Hostmaschinen Ihrer virtuellen Appliances geladen werden. Potenzielle Angreifer können dieses Protokoll ausnutzen, um Ihr System zu gefährden.

Vermeiden Sie das Laden des DCCP-Moduls, sofern dies nicht absolut notwendig ist. DCCP ist ein vorgeschlagenes Transportebenenprotokoll, das nicht verwendet wird. Wenn Sie das AppleTalk-Protokoll an den Netzwerkstapel binden, ist der Host für Angriffe anfälliger. Nicht berechnete lokale Prozesse können dazu führen, dass der Kernel einen Protokoll-Handler dynamisch lädt, indem er das Protokoll zum Öffnen eines Sockets verwendet.

Verfahren

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

- 2 Stellen Sie sicher, dass die DCCP-Zeilen in der Datei angezeigt werden.

```
install dccp/bin/true
install dccp_ipv4/bin/true
install dccp_ipv6/bin/true
```

- 3 Speichern Sie die Datei und schließen Sie sie.

Sichern der Netzwerküberbrückung

Verhindern Sie, dass das Netzwerküberbrückungs-Modul standardmäßig auf Ihrem System geladen wird. Potenzielle Angreifer können diese Überbrückung ausnutzen, um Ihr System zu gefährden.

Konfigurieren Sie Ihr System, um zu verhindern, dass das Netzwerk geladen wird, sofern dies nicht absolut notwendig ist. Potenzielle Angreifer können diese Schwachstelle ausnutzen, um die Netzwerkpartitionierung und -sicherheit zu umgehen.

Verfahren

- 1 Führen Sie den folgenden Befehl auf allen Hostmaschinen der virtuellen VMware-Appliances aus.

```
# rmmod bridge
```

- 2 Öffnen Sie die Datei `/etc/modprobe.conf.local` in einem Texteditor.
- 3 Stellen Sie sicher, dass in dieser Datei die folgende Zeile angezeigt wird.

```
install bridge /bin/false
```

- 4 Speichern Sie die Datei und schließen Sie sie.

Sichern des RDS (Reliable Datagram Sockets)-Protokolls

Im Rahmen der Härtung Ihrer Systemaktivitäten sollte das RDS-Protokoll nicht standardmäßig auf den Hostmaschinen Ihrer virtuellen Appliances geladen werden. Potenzielle Angreifer können dieses Protokoll ausnutzen, um Ihr System zu gefährden.

Wenn Sie das RDS-Protokoll an den Netzwerkstapel binden, ist der Host für Angriffe anfälliger. Nicht berechnete lokale Prozesse können dazu führen, dass das System einen Protokoll-Handler dynamisch lädt, indem er das Protokoll zum Öffnen eines Sockets verwendet.

Verfahren

- 1 Öffnen Sie die Datei `/etc/modprobe.conf.local` in einem Texteditor.
- 2 Stellen Sie sicher, dass in dieser Datei die Zeile `install rds /bin/true` angezeigt wird.
- 3 Speichern Sie die Datei und schließen Sie sie.

Sichern des TIPC (Transparent Inter-Process Communication)-Protokolls

Im Rahmen der Härtung Ihrer Systemaktivitäten sollte das TIPC-Protokoll nicht standardmäßig auf den Hostmaschinen Ihrer virtuellen Appliances geladen werden. Potenzielle Angreifer können dieses Protokoll ausnutzen, um Ihr System zu gefährden.

Wenn Sie das TIPC-Protokoll an den Netzwerkstapel binden, ist der Host für Angriffe anfälliger. Nicht berechnete lokale Prozesse können dazu führen, dass der Kernel einen Protokoll-Handler dynamisch lädt, indem er das Protokoll zum Öffnen eines Sockets verwendet.

Verfahren

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

Sichern des IPX (Internetwork Packet Exchange)-Protokolls

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

Vermeiden Sie das Laden des IPX-Protokollmoduls, sofern dies nicht absolut notwendig ist. Das IPX-Protokoll ist ein veraltetes Netzwerkschichtprotokoll. Wenn Sie das AppleTalk-Protokoll an den Netzwerkstapel binden, ist der Host für Angriffe anfälliger. Nicht berechnete lokale Prozesse können dazu führen, dass das System einen Protokoll-Handler dynamisch lädt, indem er das Protokoll zum Öffnen eines Sockets verwendet.

Verfahren

- 1 Öffnen Sie die Datei `/etc/modprobe.conf.local` in einem Texteditor.
- 2 Stellen Sie sicher, dass in dieser Datei die folgende Zeile angezeigt wird.
`install ipx /bin/true`
- 3 Speichern Sie die Datei und schließen Sie sie.

Sichern des AppleTalk-Protokolls

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

Vermeiden Sie das Laden des AppleTalk-Protokolls, sofern dies nicht absolut notwendig ist. Wenn Sie das AppleTalk-Protokoll an den Netzwerkstapel binden, ist der Host für Angriffe anfälliger. Nicht berechnete lokale Prozesse können dazu führen, dass das System einen Protokoll-Handler dynamisch lädt, indem er das Protokoll zum Öffnen eines Sockets verwendet.

Verfahren

- 1 Öffnen Sie die Datei `/etc/modprobe.conf.local` in einem Texteditor.
- 2 Stellen Sie sicher, dass in dieser Datei die folgende Zeile angezeigt wird.
`install appletalk /bin/true`
- 3 Speichern Sie die Datei und schließen Sie sie.

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 gefährden.

Vermeiden Sie das Laden des DECnet-Protokollmoduls, sofern dies nicht absolut notwendig ist. Wenn Sie das AppleTalk-Protokoll an den Netzwerkstapel binden, ist der Host für Angriffe anfälliger. Nicht berechnete lokale Prozesse können dazu führen, dass das System einen Protokoll-Handler dynamisch lädt, indem er das Protokoll zum Öffnen eines Sockets verwendet.

Verfahren

- 1 Öffnen Sie die `/etc/modprobe.conf.local`-Datei für das DECnet-Protokoll in einem Texteditor.
- 2 Stellen Sie sicher, dass in dieser Datei die folgende Zeile angezeigt wird.

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

Sichern des Firewire-Moduls

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

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

Verfahren

- 1 Öffnen Sie die Datei `/etc/modprobe.conf.local` in einem Texteditor.
- 2 Stellen Sie sicher, dass in dieser Datei die folgende Zeile angezeigt wird.

```
install ieee1394 /bin/true
```
- 3 Speichern Sie die Datei und schließen Sie sie.

Sichern der Infrastructure as a Service-Komponente

Wenn Sie Ihr System härten, sichern Sie die vRealize Automation Infrastructure as a Service (IaaS)-Komponente und die jeweilige Hostmaschine, um potenzielle Angriffe zu verhindern.

Sie müssen eine Sicherheitseinstellung für die vRealize Automation Infrastructure as a Service (IaaS)-Komponente und den jeweiligen Host konfigurieren. Sie müssen die Konfiguration von anderen zugehörigen Komponenten und Anwendungen festlegen bzw. überprüfen. In einigen Fällen können Sie die vorhandenen Einstellungen übernehmen, in anderen hingegen müssen Sie Einstellungen für eine entsprechende Konfiguration ändern bzw. hinzufügen.

Konfigurieren von NTP

Aus Sicherheitsgründen wird in einer vRealize Automation-Produktionsumgebung die Verwendung von autorisierten Zeitservern anstelle der Host-Uhrzeitsynchronisierung empfohlen.

Deaktivieren Sie in einer Produktionsumgebung die Host-Uhrzeitsynchronisierung und verwenden Sie autorisierte Zeitserver, um die präzise Verfolgung von Benutzeraktionen sowie die Identifizierung von möglicherweise böswilligen Angriffen und das Eindringen durch Überwachung und Protokollierung zu unterstützen.

Konfigurieren von TLS für Infrastructure as a Service-Data-In-Transit

Stellen Sie sicher, dass Ihre vRealize Automation-Bereitstellung starke TLS-Protokolle verwendet, um Übertragungskanäle für Infrastructure as a Service-Komponenten zu sichern.

Secure Sockets Layer (SSL) und das neuere Transport Layer Security (TLS) sind kryptografische Protokolle, die die Sicherheit des Systems während der Netzwerkkommunikation zwischen verschiedenen Systemkomponenten sicherstellen. Da SSL ein älterer Standard ist, bieten viele seiner Implementierungen keine ausreichende Sicherheit vor potenziellen Angriffen mehr. Bei früheren SSL-Protokollen einschließlich SSLv2 und SSLv3 wurden schwerwiegende Schwächen identifiziert. Diese Protokolle werden nicht mehr als sicher erachtet.

Je nach den Sicherheitsrichtlinien Ihrer Organisation ist es möglicherweise auch ratsam, TLS 1.0 zu deaktivieren.

Hinweis Deaktivieren Sie beim Beenden von TLS im Lastausgleichsdienst auch unsichere Protokolle, wie z. B. SSLv2, SSLv3 sowie gegebenenfalls TLS 1.0 und 1.1.

Aktivieren von TLS 1.1- und TLS 1.2-Protokollen für IaaS

Aktivieren und erzwingen Sie die Verwendung von TLS 1.1- und TLS 1.2-Protokollen auf allen virtuellen Maschinen, auf denen IaaS-Komponenten gehostet werden.

Verfahren

- 1 Klicken Sie auf **Start** und dann auf **Ausführen**.
- 2 Geben Sie „Regedit“ ein und klicken Sie dann auf **OK**.
- 3 Suchen Sie nach dem folgenden Registrierungsunterschlüssel und öffnen Sie ihn.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
- 4 Überprüfen Sie Folgendes und erstellen Sie gegebenenfalls neue Einträge.
 - Wenn unter „Protokolle“ kein Unterschlüssel mit der Bezeichnung „TLS 1.1“ vorhanden ist, erstellen Sie einen Unterschlüssel.
 - Wenn kein Unterschlüssel mit der Bezeichnung „Client“ unter TLS 1.1 vorhanden ist, erstellen Sie einen Unterschlüssel.
 - Wenn im Unterschlüssel des Clients kein Schlüssel mit der Bezeichnung „DisabledByDefault“ vorhanden ist, erstellen Sie einen Schlüssel vom Typ DWORD.
 - Klicken Sie mit der rechten Maustaste auf „DisabledByDefault“, wählen Sie „Bearbeiten“ aus und legen Sie den Wert auf 0 fest.

- Wenn kein Schlüssel mit der Bezeichnung „Aktiviert“ im Unterschlüssel des Clients vorhanden ist, erstellen Sie einen Schlüssel vom Typ DWORD.
 - Klicken Sie mit der rechten Maustaste auf „Aktiviert“, wählen Sie „Bearbeiten“ aus und legen Sie den Wert auf 1 fest.
 - Wenn kein Unterschlüssel mit der Bezeichnung „Server“ unter TLS 1.1 vorhanden ist, erstellen Sie einen Unterschlüssel.
 - Wenn im Unterschlüssel des Servers kein Schlüssel mit der Bezeichnung „DisabledByDefault“ vorhanden ist, erstellen Sie einen Schlüssel vom Typ DWORD.
 - Klicken Sie mit der rechten Maustaste auf „DisabledByDefault“, wählen Sie „Bearbeiten“ aus und legen Sie den Wert auf 0 fest.
 - Wenn kein Schlüssel mit der Bezeichnung „Aktiviert“ im Unterschlüssel des Servers vorhanden ist, erstellen Sie einen Schlüssel vom Typ DWORD.
 - Klicken Sie mit der rechten Maustaste auf „Aktiviert“, wählen Sie „Bearbeiten“ aus und legen Sie den Wert auf 1 fest.
- 5 Wiederholen Sie die vorhergehenden Schritte für das TLS 1.2-Protokoll.

Hinweis Um die Nutzung von TLS 1.1 und 1.2 zu erzwingen, sind zusätzliche Einstellungen notwendig, die in den folgenden Schritten beschrieben werden.

- 6 Suchen Sie nach dem folgenden Registrierungsunterschlüssel und öffnen Sie ihn.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319

- 7 Überprüfen Sie Folgendes und erstellen Sie gegebenenfalls neue Einträge.

- Wenn kein DWORD-Eintrag mit der Bezeichnung „SchUseStrongCrypto“ vorhanden ist, erstellen Sie ihn und legen Sie den zugehörigen Wert auf 1 fest.
- Wenn kein DWORD-Eintrag mit der Bezeichnung „SystemDefaultTlsVersions“ vorhanden ist, erstellen Sie ihn und legen Sie den zugehörigen Wert auf 1 fest.

- 8 Suchen Sie nach dem folgenden Registrierungsunterschlüssel und öffnen Sie ihn.

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v4.0.30319

- 9 Überprüfen Sie Folgendes und erstellen Sie gegebenenfalls neue Einträge.

- Wenn kein DWORD-Eintrag mit der Bezeichnung „SchUseStrongCrypto“ vorhanden ist, erstellen Sie ihn und legen Sie den zugehörigen Wert auf 1 fest.
- Wenn kein DWORD-Eintrag mit der Bezeichnung „SystemDefaultTlsVersions“ vorhanden ist, erstellen Sie ihn und legen Sie den zugehörigen Wert auf 1 fest.

Deaktivieren von SSL 3.0 und TLS 1.0 für IaaS

Deaktivieren Sie SSL 3.0 und das veraltete TLS 1.0-Protokoll für IaaS-Komponenten.

Verfahren

1 Klicken Sie auf **Start** und dann auf **Ausführen**.

2 Geben Sie Regedit ein und klicken Sie dann auf **OK**.

3 Suchen Sie nach dem folgenden Registrierungsunterschlüssel und öffnen Sie ihn.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SChannel\Protocols

4 Überprüfen Sie Folgendes und erstellen Sie gegebenenfalls neue Einträge.

- Wenn unter „Protokolle“ kein Unterschlüssel mit der Bezeichnung „SSL 3.0“ vorhanden ist, erstellen Sie einen Unterschlüssel.
- Wenn kein Unterschlüssel mit der Bezeichnung „Client“ unter SSL 3.0 vorhanden ist, erstellen Sie einen Unterschlüssel.
- Wenn im Unterschlüssel des Clients kein Schlüssel mit der Bezeichnung „DisabledByDefault“ vorhanden ist, erstellen Sie einen Schlüssel vom Typ DWORD.
- Klicken Sie mit der rechten Maustaste auf „DisabledByDefault“, wählen Sie „Bearbeiten“ aus und legen Sie den Wert auf 1 fest.
- Klicken Sie mit der rechten Maustaste auf „Aktiviert“, wählen Sie „Bearbeiten“ aus und legen Sie den Wert auf 0 fest.
- Wenn kein Unterschlüssel mit der Bezeichnung „Server“ unter SSL 3.0 vorhanden ist, erstellen Sie einen Unterschlüssel.
- Wenn im Unterschlüssel des Servers kein Schlüssel mit der Bezeichnung „DisabledByDefault“ vorhanden ist, erstellen Sie einen Schlüssel vom Typ DWORD.
- Klicken Sie mit der rechten Maustaste auf „DisabledByDefault“, wählen Sie „Bearbeiten“ aus und legen Sie den Wert auf 1 fest.
- Wenn kein Schlüssel mit der Bezeichnung „Auf dem Server aktiviert“ vorhanden ist, erstellen Sie einen Schlüssel vom Typ DWORD.
- Klicken Sie mit der rechten Maustaste auf „Aktiviert“, wählen Sie „Bearbeiten“ aus und legen Sie den Wert auf 0 fest.

5 Wiederholen Sie die vorhergehenden Schritte für das TLS 1.0-Protokoll.

Deaktivieren von TLS 1.0 für IaaS

Um maximale Sicherheit zu bieten, konfigurieren Sie IaaS zur Verwendung von Pooling und deaktivieren Sie TLS 1.0.

Weitere Informationen finden Sie im Microsoft-Knowledgebase-Artikel unter <https://support.microsoft.com/en-us/kb/245030>.

Verfahren

1 Konfigurieren Sie IaaS zur Verwendung von Pooling anstelle von Web-Sockets.

- a Aktualisieren Sie die Manager Services-Konfigurationsdatei C:\Programme (x86)\VMware\VCAC\Server\ManagerService.exe.config, indem Sie die folgenden Werte im <appSettings>-Abschnitt hinzufügen.

```
<add key="Extensibility.Client.RetrievalMethod" value="Polling"/>
<add key="Extensibility.Client.PollingInterval" value="2000"/>
<add key="Extensibility.Client.PollingMaxEvents" value="128"/>
```

- b Starten Sie den Manager Service (VMware vCloud Automation Center Service) neu.

2 Vergewissern Sie sich, dass TLS 1.0 auf dem IaaS-Server deaktiviert ist.

- a Führen Sie den Registrierungs-Editor als Administrator aus.
- b Navigieren Sie im Registrierungsfenster zu HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\.
- c Klicken Sie mit der rechten Maustaste auf „Protokolle“, wählen Sie **Neu > Schlüssel** aus und geben Sie **TLS 1.0** ein.
- d Klicken Sie in der Navigationsstruktur mit der rechten Maustaste auf den TLS 1.0-Schlüssel, den Sie gerade erstellt haben, wählen Sie im Popup-Menü **Neu > Schlüssel** aus und geben Sie **Client** ein.
- e Klicken Sie in der Navigationsstruktur mit der rechten Maustaste auf den TLS 1.0-Schlüssel, den Sie gerade erstellt haben, wählen Sie im Popup-Menü **Neu > Schlüssel** aus und geben Sie **Server** ein.
- f Klicken Sie in der Navigationsstruktur unter „TLS 1.0“ mit der rechten Maustaste auf **Client**, klicken Sie auf **Neu > DWORD-Wert (32-Bit)** und geben Sie **DisabledByDefault** ein.
- g Wählen Sie in der Navigationsstruktur unter „TLS 1.0“ die Option **Client** aus, doppelklicken Sie im rechten Bereich auf **DisabledByDefault** DWORD und geben Sie **1** ein.
- h Klicken Sie in der Navigationsstruktur unter „TLS 1.0“ mit der rechten Maustaste auf **Server**, wählen Sie **Neu > DWORD-Wert (32-Bit)** aus und geben Sie **Enabled** ein.
- i Wählen Sie in der Navigationsstruktur unter „TLS 1.0“ die Option **Server** aus, doppelklicken Sie im rechten Bereich auf das DWORD **Aktiviert** und geben Sie **0** ein.
- j Starten Sie den Windows-Server neu.

Konfigurieren von TLS-Verschlüsselungs-Suites

Für maximale Sicherheit müssen Sie vRealize Automation-Komponenten für die Verwendung starker Verschlüsselungen konfigurieren. Die zwischen dem Server und dem Browser ausgehandelte Verschlüsselungsschlüsselstärke bestimmt die Verschlüsselungsstärke, die in einer TLS-Sitzung verwendet wird. Um sicherzustellen, dass nur starke Verschlüsselungen ausgewählt werden, deaktivieren Sie schwache Verschlüsselungen in vRealize Automation-Komponenten. Konfigurieren Sie den Server so, dass er nur

starke Verschlüsselungen unterstützt und ausreichend große Schlüsselgrößen verwendet. Konfigurieren Sie außerdem alle Verschlüsselungen in einer geeigneten Reihenfolge.

Nicht akzeptable Verschlüsselungs-Suites

Deaktivieren Sie Verschlüsselungs-Suites, die keine Authentifizierung bieten, wie NULL-Verschlüsselungs-Suites, aNULL oder eNULL. Deaktivieren Sie auch anonymen Diffie-Hellman-Schlüsselaustausch (ADH), Export Level Cipher-Instanzen (EXP, Verschlüsselungen, die DES enthalten), Schlüsselgrößen unter 128 Bit für die Verschlüsselung von Nutzlast-Datenverkehr, die Verwendung von MD5 als Hashing-Mechanismus für Nutzlast-Datenverkehr, IDEA-Verschlüsselungs-Suites und RC4-Verschlüsselungs-Suites. Stellen Sie außerdem sicher, dass Verschlüsselungs-Suites, die den Diffie-Hellman (DHE)-Schlüsselaustausch verwenden, deaktiviert sind.

Informationen zur Deaktivierung statischer Verschlüsselung mit Schlüsseln in vRealize Automation finden Sie im [Knowledgebase-Artikel 71094](#).

Überprüfen der Hostserver-Sicherheit

Aus Sicherheitsgründen wird empfohlen, die Konfiguration der Sicherheit auf Ihren IaaS (Infrastructure as a Service)-Hostserver-Maschinen zu überprüfen.

Microsoft bietet verschiedene Tools zum Überprüfen der Sicherheit auf Hostserver-Maschinen. Hilfestellung für den Einsatz dieser Tools erhalten Sie von Ihrem Microsoft-Anbieter.

Überprüfen der sicheren Baseline für Hostserver

Mit dem Microsoft Baseline Security Analyzer (MBSA) können Sie schnell feststellen, ob Ihr Server über die neuesten Aktualisierungen oder Hotfixes verfügt. Sie können den MBSA zum Installieren von fehlenden Microsoft-Sicherheitspatches verwenden, um Ihren Server mit den neuesten Sicherheitsempfehlungen von Microsoft auf dem neuesten Stand zu halten.

Laden Sie die neueste Version des MBSA-Tools von der Microsoft-Website herunter.

Überprüfen der Sicherheitskonfiguration der Hostserver

Verwenden Sie den Windows-Sicherheitskonfigurations-Assistenten (Windows Security Configuration Wizard, SCW) und das Microsoft Security Compliance Manager (SCM)-Toolkit, um sicherzustellen, dass der Hostserver sicher konfiguriert ist.

Führen Sie den SCW unter Verwendung des Verwaltungstools Ihres Windows-Servers aus. Mit diesem Tool können die Rollen Ihres Servers sowie die installierten Funktionen, einschließlich Netzwerk, Windows-Firewalls und Registrierungseinstellungen, identifiziert werden. Vergleichen Sie den Bericht mit den aktuellen Anweisungen zur Härtung aus dem entsprechenden SCM für Ihren Windows-Server. Basierend auf den Ergebnissen können Sie eine Feinabstimmung der Sicherheitseinstellungen für jede Funktion vornehmen (wie zum Beispiel für Netzwerkdienste, Kontoeinstellungen und Windows-Firewalls) und die Einstellungen auf Ihren Server anwenden.

Weitere Informationen zum SCW-Tool finden Sie auf der Microsoft Technet-Website.

Schützen von Anwendungsressourcen

Stellen Sie aus Sicherheitsgründen sicher, dass alle relevanten Infrastructure as a Service-Dateien über die entsprechenden Berechtigungen verfügen.

Überprüfen Sie Infrastructure as a Service-Dateien in Ihrer Infrastructure as a Service-Installation. In den meisten Fällen stimmen die Unterordner und Dateien für alle Ordner mit den Einstellungen des Ordners überein.

Verzeichnis oder Datei	Gruppe oder Benutzer	Vollständige Kontrolle	Ändern	Lesen und ausführen	Lesen	Schreiben
VMware\VCAC\Agents \<agent_name>\logs	System	X	X	X	X	X
	Administrator	X	X	X	X	X
	Administratoren	X	X	X	X	X
VMware\VCAC\Agents \<agent_name>\temp	System	X	X	X	X	X
	Administrator	X	X	X	X	X
	Administratoren	X	X	X	X	X
VMware\VCAC\Agents\	System	X	X	X	X	X
	Administratoren	X	X	X	X	X
	Benutzer			X	X	
VMware\VCAC\Distributed Execution Manager\	System	X	X	X	X	X
	Administratoren	X	X	X	X	X
	Benutzer			X	X	
VMware\VCAC\Distributed Execution Manager\DEM\Logs	System	X	X	X	X	X
	Administrator	X	X	X	X	X
	Administratoren	X	X	X	X	X
VMware\VCAC\Distributed Execution Manager\DEO\Logs	System	X	X	X	X	X
	Administrator	X	X	X	X	X
	Administratoren	X	X	X	X	X
VMware\VCAC\Management Agent\	System	X	X	X	X	X
	Administratoren	X	X	X	X	X
	Benutzer			X	X	
VMware\VCAC\Server\	System	X	X	X	X	X
	Administratoren	X	X	X	X	X
	Benutzer			X	X	
VMware\VCAC\Web API	System	X	X	X	X	X
	Administratoren	X	X	X	X	X
	Benutzer			X	X	

Sichern der Infrastructure as a Service-Hostmaschine

Überprüfen Sie als Best Practice im Hinblick auf die Sicherheit die allgemeinen Einstellungen auf Ihrer Infrastructure as a Service (IaaS)-Hostmaschine, um sicherzustellen, dass sie den Sicherheitsrichtlinien entspricht.

Sichern Sie sonstige Konten, Anwendungen, Ports und Dienste auf der Infrastructure as a Service (IaaS)-Hostmaschine.

Überprüfen der Benutzerkontoeinstellungen des Servers

Stellen Sie sicher, dass keine unnötigen lokalen und Domänenbenutzerkonten und -Einstellungen vorhanden sind. Beschränken Sie alle Benutzerkonten, die nicht im Zusammenhang mit den Funktionen der Anwendung stehen, auf diejenigen, die für die Verwaltung, Wartung und Fehlerbehebung erforderlich sind. Beschränken Sie den Remotezugriff über Domänenbenutzerkonten auf das erforderliche Mindestmaß für die Wartung des Servers. Kontrollieren und prüfen Sie diese Konten genau.

Löschen unnötiger Anwendungen

Löschen Sie alle nicht benötigten Anwendungen von den Hostservern. Nicht benötigte Anwendungen erhöhen das Risiko einer Offenlegung aufgrund ihrer unbekannten oder unbehobenen Schwachstellen.

Deaktivieren unnötiger Ports und Dienste

Überprüfen Sie die Hostserver-Firewall auf die Liste offener Ports. Blockieren Sie alle Ports, die für die IaaS-Komponente oder den kritischen Systemvorgang nicht erforderlich sind. Siehe [Konfigurieren von Ports und Protokollen](#). Überwachen Sie die Dienste, die für Ihren Hostserver ausgeführt werden, und deaktivieren Sie all jene, die nicht benötigt werden.

Konfigurieren der Hostnetzwerksicherheit

8

Um maximalen Schutz vor bekannten Sicherheitsrisiken zu ermöglichen, konfigurieren Sie Einstellungen für die Netzwerkschnittstelle und Kommunikation auf allen VMware-Hostmaschinen.

Konfigurieren Sie im Rahmen eines umfassenden Sicherheitsplans die Einstellungen für die Sicherheit der Netzwerkschnittstelle für die virtuellen VMware-Appliances und die Infrastructure as a Service-Komponenten gemäß den festgelegten Sicherheitsrichtlinien.

Dieses Kapitel enthält die folgenden Themen:

- [Konfigurieren von Netzwerkeinstellungen für VMware-Appliances](#)
- [Konfigurieren von Netzwerkeinstellungen für den Infrastructure as a Service-Host](#)
- [Konfigurieren von Ports und Protokollen](#)

Konfigurieren von Netzwerkeinstellungen für VMware-Appliances

Um sicherzustellen, dass die Hostmaschinen der virtuellen VMware-Appliance nur sichere und wichtige Kommunikation unterstützen, überprüfen und bearbeiten Sie deren Einstellungen für die Netzwerkkommunikation.

Überprüfen Sie die Netzwerk-IP-Protokollkonfiguration der VMware-Hostmaschine und konfigurieren Sie die Netzwerkeinstellungen gemäß den Sicherheitsrichtlinien. Deaktivieren Sie alle nicht benötigten Kommunikationsprotokolle.

Verhindern der Benutzerkontrolle von Netzwerkschnittstellen

Aus Sicherheitsgründen wird empfohlen, Benutzern nur die Systemberechtigungen zu gewähren, die sie für ihre Arbeit auf den Hostmaschinen der VMware-Appliances benötigen.

Das Zulassen der Bearbeitung von Netzwerkschnittstellen durch Benutzerkonten kann zur Umgehung von Sicherheitsmechanismen für das Netzwerk oder zum Denial-of-Service führen. Beschränken Sie das Ändern der Einstellungen von Netzwerkschnittstellen auf berechtigte Benutzer.

Verfahren

- 1 Führen Sie den folgenden Befehl auf allen Hostmaschinen der VMware-Appliances aus.

```
# grep -i '^USERCONTROL=' /etc/sysconfig/network/ifcfg*
```

- 2 Stellen Sie sicher, dass jede Schnittstelle auf NO festgelegt ist.

Festlegen der Warteschlangengröße für TCP-Backlogs

Um eine bestimmte Verteidigungsebene gegen Angriffe bereitzustellen, konfigurieren Sie eine Standardwarteschlangengröße für TCP-Backlogs auf den Hostmaschinen der VMware-Appliances.

Legen Sie die Warteschlangengröße für TCP-Backlogs auf einen entsprechenden Standardwert fest, um das Risiko von TCP-Denial-of-Service-Angriffen zu minimieren. Die empfohlene Standardeinstellung ist 1280.

Verfahren

- 1 Führen Sie den folgenden Befehl auf allen Hostmaschinen der VMware-Appliances durch.

```
# cat /proc/sys/net/ipv4/tcp_max_syn_backlog
```

- 2 Öffnen Sie die Datei `/etc/sysctl.conf` mit einem Texteditor.
- 3 Legen Sie die Standardwarteschlangengröße für TCP-Backlogs fest, indem Sie der Datei den folgenden Eintrag hinzufügen.

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

- 4 Speichern Sie die Änderungen und schließen Sie die Datei.

Verweigern von ICMPv4-Echos für Broadcast-Adressen

Stellen Sie als Best Practice im Hinblick auf die Sicherheit sicher, dass die Hostmaschinen der VMware-Appliance Anforderungen für ICMP-Broadcast-Adressen-Echos ignorieren.

Antworten auf Broadcast-Internet Control Message Protocol (ICMP)-Echos bieten einen Angriffspunkt für Verstärkungsangriffe und können die Netzwerkzuordnung durch bösartige Agents erleichtern. Wenn Sie die Hostmaschinen der Appliance so konfigurieren, dass ICMPv4-Echos ignoriert werden, wird ein Schutz vor solchen Angriffen geboten.

Verfahren

- 1 Führen Sie den `# cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts`-Befehl auf den Hostmaschinen der virtuellen VMware-Appliance aus, um zu bestätigen, dass sie Anforderungen für IPv4-Broadcast-Adressen-Echos ablehnen.

Wenn die Hostmaschinen für die Ablehnung von IPv4-Umleitungen konfiguriert sind, gibt dieser Befehl einen Wert von 0 für `/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts` zurück.

- 2 Um die Hostmaschine einer virtuellen Appliance für die Ablehnung von Anforderungen für ICMPv4-Broadcast-Adressen-Echos zu konfigurieren, öffnen Sie die Datei `/etc/sysctl.conf` auf Windows-Hostmaschinen in einem Texteditor.
- 3 Suchen Sie nach dem Eintrag `net.ipv4.icmp_echo_ignore_broadcasts=0`. Wenn der Wert für diesen Eintrag nicht auf 0 gesetzt oder der Eintrag nicht vorhanden ist, fügen Sie ihn hinzu oder aktualisieren den vorhandenen Eintrag entsprechend.
- 4 Speichern Sie die Änderungen und schließen Sie die Datei.

Deaktivieren von IPv4 Proxy ARP

Stellen Sie sicher, dass IPv4 Proxy ARP deaktiviert ist, falls die Aktivierung auf den Hostmaschinen Ihrer VMware-Appliance nicht erforderlich ist, um die nicht autorisierte Freigabe von Informationen zu verhindern.

Mit IPv4 Proxy ARP kann ein System Antworten auf ARP-Anfragen im Namen von verbundenen Hosts von einer Schnittstelle an eine andere Schnittstelle senden. Deaktivieren Sie die Funktion, falls nicht erforderlich, um die Weitergabe von Adressinformationen zwischen den angehängten Netzwerksegmenten zu verhindern.

Verfahren

- 1 Führen Sie den `# grep [01] /proc/sys/net/ipv4/conf/*/proxy_arp | egrep "default|all"`-Befehl auf den Hostmaschinen der virtuellen VMware-Appliance aus, um sicherzustellen, dass IPv4 Proxy ARP deaktiviert ist.

Wenn auf den Hostmaschinen IPv6 Proxy ARP deaktiviert ist, gibt dieser Befehl Werte von 0 zurück.

```
/proc/sys/net/ipv4/conf/all/proxy_arp:0
/proc/sys/net/ipv4/conf/default/proxy_arp:0
```

Wenn die Hostmaschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Wenn Sie IPv6 Proxy ARP auf Hostmaschinen konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
- 3 Überprüfen Sie die folgenden Einträge.

```
net.ipv4.conf.default.proxy_arp=0
net.ipv4.conf.all.proxy_arp=0
```

Wenn die Einträge nicht vorhanden sind oder deren Werte nicht auf Null gesetzt sind, fügen Sie die Einträge hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

- 4 Speichern Sie alle von Ihnen vorgenommenen Änderungen und schließen Sie die Datei.

Verweigern von IPv4-ICMP-Umleitungsmeldungen

Stellen Sie als Best Practice im Hinblick auf die Sicherheit sicher, dass die Hostmaschinen der virtuellen VMware-Appliance IPv4-ICMP-Umleitungsmeldungen ablehnen.

Router verwenden ICMP-Umleitungsmeldungen, um Hosts mitzuteilen, dass für ein Ziel eine direktere Route vorhanden ist. Eine bösartige ICMP-Umleitungsmeldung kann einen Man-in-the-Middle-Angriff erleichtern. Diese Meldungen ändern die Routentabelle des Hosts und sind nicht authentifiziert. Stellen Sie sicher, dass das System so konfiguriert ist, dass diese ignoriert werden, wenn sie ansonsten nicht benötigt werden.

Verfahren

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv4/conf/*/accept_redirects | egrep "default|all"` auf den Hostmaschinen der VMware-Appliance aus, um zu bestätigen, dass sie IPv4-Umleitungsmeldungen verweigern.

Dieser Befehl gibt Folgendes zurück, wenn die Hostmaschinen für die Verweigerung von IPv4-Umleitungsmeldungen konfiguriert sind:

```
/proc/sys/net/ipv4/conf/all/accept_reidrects:0
```

```
/proc/sys/net/ipv4/conf/default/accept_redirects:0
```

- 2 Wenn Sie eine Hostmaschine der virtuellen Appliance für die Verweigerung von IPv4-Umleitungsmeldungen konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.

- 3 Überprüfen Sie die Werte der Zeilen, die mit `net.ipv4.conf` beginnen.

Wenn die Werte für die folgenden Einträge nicht auf Null gesetzt sind oder wenn die Einträge nicht vorhanden sind, fügen Sie sie zur Datei hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

```
net.ipv4.conf.all.accept_redirects=0
net.ipv4.conf.default.accept_redirects=0
```

- 4 Speichern Sie die von Ihnen vorgenommenen Änderungen und schließen Sie die Datei.

Verweigern von IPv6-ICMP-Umleitungsmeldungen

Stellen Sie als Best Practice für Sicherheit sicher, dass die Hostmaschinen Ihrer virtuellen VMware-Appliance IPv6-ICMP-Umleitungsmeldungen verweigern.

Router verwenden ICMP-Umleitungsmeldungen, um Hosts mitzuteilen, dass für ein Ziel eine direktere Route vorhanden ist. Eine bössartige ICMP-Umleitungsmeldung kann einen Man-in-the-Middle-Angriff erleichtern. Diese Meldungen ändern die Routentabelle des Hosts und sind nicht authentifiziert. Stellen Sie sicher, dass Ihr System so konfiguriert ist, dass diese Meldungen ignoriert werden (falls nicht anderweitig erforderlich).

Verfahren

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv6/conf/*/accept_redirects | egrep "default|all"` auf den Hostmaschinen der virtuellen VMware-Appliance aus, um zu bestätigen, dass IPv6-Umleitungsmeldungen verweigert werden.

Wenn die Hostmaschinen für die Verweigerung von IPv6-Umleitungsmeldungen konfiguriert sind, gibt dieser Befehl Folgendes zurück:

```
/proc/sys/net/ipv6/conf/all/accept_redirects:0
```

```
/proc/sys/net/ipv6/conf/default/accept_redirects:0
```

- 2 Um eine Hostmaschine der virtuellen Appliance zum Verweigern von IPv4-Umleitungsmeldungen zu konfigurieren, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
- 3 Überprüfen Sie die Werte der Zeilen, die mit `net.ipv6.conf` beginnen.

Wenn die Werte für die folgenden Einträge nicht auf Null gesetzt oder die Einträge nicht vorhanden sind, fügen Sie sie zur Datei hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

```
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```

- 4 Speichern Sie die Änderungen und schließen Sie die Datei.

Protokollieren von IPv4-Martian-Paketen

Stellen Sie als Best Practice für Sicherheit sicher, dass die Hostmaschinen Ihrer virtuellen VMware-Appliance IPv4-Martian-Pakete protokollieren.

Martian-Pakete enthalten Adressen, die das System als ungültig erkennt. Konfigurieren Sie Ihre Hostcomputer zur Protokollierung dieser Meldungen, damit Sie falsche Konfigurationen oder laufende Angriffe identifizieren können.

Verfahren

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv4/conf/*/log_martians | grep "default|all"` auf den Hostmaschinen der VMware-Appliance aus, um sicherzustellen, dass IPv4-Martian-Pakete protokolliert werden.

Wenn die virtuellen Maschinen zum Konfigurieren von Martian-Paketen konfiguriert sind, geben sie Folgendes zurück:

```
/proc/sys/net/ipv4/conf/all/log_martians:1
/proc/sys/net/ipv4/conf/default/log_martians:1
```

Wenn die Hostmaschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Wenn Sie die virtuellen Maschinen zum Konfigurieren von IPv4-Martian-Paketen konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
- 3 Überprüfen Sie die Werte der Zeilen, die mit `net.ipv4.conf` beginnen.

Wenn der Wert der folgenden Einträge nicht auf 1 gesetzt ist oder die Werte nicht vorhanden sind, fügen Sie sie zur Datei hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

```
net.ipv4.conf.all.log_martians=1
net.ipv4.conf.default.log_martians=1
```

- 4 Speichern Sie die Änderungen und schließen Sie die Datei.

Verwenden der IPv4 Reverse Path-Filterung

Stellen Sie als Best Practice im Hinblick auf die Sicherheit sicher, dass die Hostmaschinen der virtuellen VMware-Appliance IPv4 Reverse Path-Filterung verwenden.

Reverse Path-Filterung schützt vor manipulierten Quelladressen, indem das System Pakete mit Quelladressen verwirft, die über keine Route oder eine Route verfügen, die nicht auf die ursprüngliche Schnittstelle verweist. Konfigurieren Sie Ihre Hostmaschinen für die Verwendung von Reverse Path-Filterung wann immer möglich. In einigen Fällen, je nach Systemrolle, kann Reverse Path-Filterung bewirken, dass das System legitimen Datenverkehr verwirft. Wenn solche Probleme auftreten, müssen Sie möglicherweise einen weniger strengen Modus verwenden oder Reverse Path-Filterung vollständig deaktivieren.

Verfahren

- 1 Führen Sie den `# grep [01] /proc/sys/net/ipv4/conf/*/rp_filter | egrep "default|all"` -Befehl auf den Hostmaschinen der virtuellen VMware-Appliance aus, um sicherzustellen, dass IPv4 Reverse Path-Filterung verwendet wird.

Dieser Befehl gibt Folgendes zurück, wenn die virtuellen Maschinen IPv4 Reverse Path-Filterung verwenden:

```
/proc/sys/net/ipv4/conf/all/rp_filter:1
/proc/sys/net/ipv4/conf/default/re_filter:1
```

Wenn Ihre virtuellen Maschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Wenn Sie IPv4 Reverse Path-Filterung auf Hostmaschinen konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
- 3 Überprüfen Sie die Werte der Zeilen, die mit `net.ipv4.conf` beginnen.

Wenn die Werte für die folgenden Einträge nicht auf 1 gesetzt oder nicht vorhanden sind, fügen Sie sie der Datei hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

```
net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.default.rp_filter=1
```

- 4 Speichern Sie die Änderungen und schließen Sie die Datei.

Verweigern der IPv4-Weiterleitung

Stellen Sie sicher, dass die Hostmaschinen der VMware-Appliance die IPv4-Weiterleitung verweigern.

Wenn das System für die IP-Weiterleitung konfiguriert ist und kein designierter Router ist, könnten Angreifer es nutzen, um die Netzwerksicherheit zu umgehen, indem sie einen Pfad für die Kommunikation, die nicht von Netzwerkgeräten gefiltert wird, bereitstellen. Konfigurieren Sie die Hostmaschinen der virtuellen Appliance so, dass die IPv4-Weiterleitung verweigert wird, um dieses Risiko zu vermeiden.

Verfahren

- 1 Führen Sie den Befehl `# cat /proc/sys/net/ipv4/ip_forward` auf den Hostmaschinen der VMware-Appliance aus, um zu bestätigen, dass sie die IPv4-Weiterleitung verweigern.

Wenn die Hostmaschinen so konfiguriert sind, dass sie die IPv4-Weiterleitung verweigern, gibt dieser Befehl einen Wert von 0 für `/proc/sys/net/ipv4/ip_forward` zurück. Wenn die virtuellen Maschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Um die Hostmaschine der virtuellen Appliance für das Verweigern der IPv4-Weiterleitung zu konfigurieren, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
- 3 Suchen Sie nach dem Eintrag `net.ipv4.ip_forward=0`. Wenn der Wert für diesen Eintrag derzeit nicht auf Null gesetzt ist oder wenn der Eintrag nicht vorhanden ist, fügen Sie ihn hinzu oder aktualisieren Sie den vorhandenen Eintrag entsprechend.
- 4 Speichern Sie die Änderungen und schließen Sie die Datei.

Verweigern der IPv6-Weiterleitung

Stellen Sie als Best Practice im Hinblick auf die Sicherheit sicher, dass die VMware-Appliance-Hostsysteme die IPv6-Weiterleitung verweigern.

Wenn das System für die IP-Weiterleitung konfiguriert ist und kein designierter Router ist, könnten Angreifer es nutzen, um die Netzwerksicherheit zu umgehen, indem sie einen Pfad für die Kommunikation, die nicht von Netzwerkgeräten gefiltert wird, bereitstellen. Konfigurieren Sie die Hostmaschinen der virtuellen Appliance für die Verweigerung der IPv6-Weiterleitung, um dieses Risiko zu vermeiden.

Verfahren

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv6/conf/*/forwarding | grep "default|all"` auf den Hostmaschinen der VMware-Appliance aus, um sicherzustellen, dass sie die IPv6-Weiterleitung ablehnen.

Wenn die Hostmaschinen für die Verweigerung der IPv6-Weiterleitung konfiguriert sind, gibt dieser Befehl Folgendes zurück:

```
/proc/sys/net/ipv6/conf/all/forwarding:0
/proc/sys/net/ipv6/conf/default/forwarding:0
```

Wenn die Hostmaschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Wenn Sie eine Hostmaschine für die Verweigerung der IPv6-Weiterleitung konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.

- 3 Überprüfen Sie die Werte der Zeilen, die mit `net.ipv6.conf` beginnen.

Wenn die Werte für die folgenden Einträge nicht auf Null gesetzt sind oder wenn die Einträge nicht vorhanden sind, fügen Sie die Einträge hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

```
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```

- 4 Speichern Sie alle von Ihnen vorgenommenen Änderungen und schließen Sie die Datei.

Verwenden von IPv4-TCP Syncookies

Stellen Sie sicher, dass die Hostmaschinen Ihrer VMware-Appliance IPv4-TCP Syncookies verwenden.

Ein TCP SYN-Flutangriff führt möglicherweise zu einem Denial-of-Service, indem die TCP-Verbindungstabelle eines Systems mit Verbindungen im SYN_RCVD-Status aufgefüllt wird. Syncookies verhindern das Nachverfolgen einer Verbindung bis zum Erhalt einer nachfolgenden Quittierung und stellen sicher, dass der Initiator eine gültige Verbindung herstellt und keine Flutquelle ist. Dieses Verfahren funktioniert nicht in einer vollständigen Übereinstimmung mit den Standards. Es wird daher nur während einer Flutbedingung eingesetzt und ermöglicht die Absicherung des Systems bei fortwährender Verarbeitung von Anforderungen.

Verfahren

- 1 Führen Sie den `# cat /proc/sys/net/ipv4/tcp_syncookies`-Befehl auf den Hostmaschinen der VMware-Appliances aus, um sicherzustellen, dass IPv4-TCP Syncookies verwendet werden.

Wenn die Hostmaschinen zum Ablehnen der IPv4-Weiterleitung konfiguriert sind, gibt dieser Befehl einen Wert von 1 für `/proc/sys/net/ipv4/tcp_syncookies` zurück. Wenn die virtuellen Maschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Wenn Sie eine virtuelle Appliance zur Verwendung von IPv4-TCP Syncookies konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.

- 3 Suchen Sie nach dem Eintrag `net.ipv4.tcp_syncookies=1`.

Wenn der Wert für diesen Eintrag aktuell nicht auf 1 festgelegt oder nicht vorhanden ist, fügen Sie den Eintrag hinzu oder aktualisieren Sie den vorhandenen Eintrag entsprechend.

- 4 Speichern Sie alle von Ihnen vorgenommenen Änderungen und schließen Sie die Datei.

Verweigern von IPv6-Routerankündigungen

Stellen Sie sicher, dass die VMware-Hostmaschinen die Annahme von Routerankündigungen und ICMP-Redirects verweigern, sofern nicht anderweitig für den Systembetrieb benötigt.

Mit IPv6 können Systeme ihre Netzwerkgeräte durch die automatische Verwendung von Informationen aus dem Netzwerk konfigurieren. Aus Sicherheitsgründen ist das manuelle Konfigurieren wichtiger Konfigurationsinformationen deren Annahme über das Netzwerk in einer nicht authentifizierten Art und Weise vorzuziehen.

Verfahren

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra | grep "default|all"` auf den Hostmaschinen der VMware-Appliance aus, um sicherzustellen, dass sie die Routerankündigungen verweigern.

Wenn die Hostmaschinen für die Verweigerung von IPv6 Routerankündigungen konfiguriert sind, gibt dieser Befehl Werte von 0 zurück:

```
/proc/sys/net/ipv6/conf/all/accept_ra:0
/proc/sys/net/ipv6/conf/default/accept_ra:0
```

Wenn die Hostmaschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Wenn Sie eine Hostmaschine für die Verweigerung von IPv6-Routerankündigungen konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
- 3 Überprüfen Sie die folgenden Einträge.

```
net.ipv6.conf.all.accept_ra=0
net.ipv6.conf.default.accept_ra=0
```

Wenn diese Einträge nicht vorhanden sind oder ihre Werte nicht auf Null gesetzt sind, fügen Sie die Einträge hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

- 4 Speichern Sie alle von Ihnen vorgenommenen Änderungen und schließen Sie die Datei.

Verweigern von IPv6-Routeranfragen

Stellen Sie als Best Practice im Hinblick auf die Sicherheit sicher, dass die Hostmaschinen der VMware-Appliance IPv6-Routeranfragen ablehnen, es sei denn, sie sind für den Systembetrieb erforderlich.

Die Einstellung der Routeranfragen bestimmt, wie viele Routeranfragen beim Anzeigen der Schnittstelle gesendet werden. Wenn Adressen statisch zugewiesen werden, ist es nicht erforderlich, Anfragen zu senden.

Verfahren

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv6/conf/*/router_solicitations | grep "default|all"` auf den Hostmaschinen der VMware-Appliance aus, um sicherzustellen, dass sie IPv6-Routeranfragen ablehnen.

Wenn die Hostmaschinen für die Verweigerung der IPv6-Routerankündigungen konfiguriert sind, gibt dieser Befehl Folgendes zurück:

```
/proc/sys/net/ipv6/conf/all/router_solicitations:0
/proc/sys/net/ipv6/conf/default/router_solicitations:0
```

Wenn die Hostmaschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Wenn Sie Hostmaschinen für die Verweigerung von IPv6-Routeranfragen konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
- 3 Überprüfen Sie die folgenden Einträge.

```
net.ipv6.conf.all.router_solicitations=0
net.ipv6.conf.default.router_solicitations=0
```

Wenn die Einträge nicht vorhanden sind oder deren Werte nicht auf Null gesetzt sind, fügen Sie die Einträge hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

- 4 Speichern Sie die Änderungen und schließen Sie die Datei.

Verweigern der IPv6 Routereinstellungen bei Routeranfragen

Stellen Sie sicher, dass die Hostmaschinen der VMware-Appliance IPv6-Routeranfragen ablehnen, es sei denn, sie sind für den Systembetrieb erforderlich.

Die Routereinstellungen in der Anfrageneinstellung bestimmen die Routereinstellungen. Wenn Adressen statisch zugewiesen werden, ist es nicht erforderlich, Routereinstellungen für Anfragen zu empfangen.

Verfahren

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_rtr_pref | egrep "default|all"` auf den Hostmaschinen der VMware-Appliance aus, um sicherzustellen, dass sie IPv6-Routeranfragen ablehnen.

Wenn die Hostmaschinen für die Verweigerung der IPv6-Routerankündigungen konfiguriert sind, gibt dieser Befehl Folgendes zurück:

```
/proc/sys/net/ipv6/conf/all/accept_ra_rtr_pref:0
/proc/sys/net/ipv6/conf/default/accept_ra_rtr_pref:0
```

Wenn die Hostmaschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Wenn Sie Hostmaschinen für die Verweigerung von IPv6-Routeranfragen konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
- 3 Überprüfen Sie die folgenden Einträge.

```
net.ipv6.conf.all.accept_ra_rtr_pref=0
net.ipv6.conf.default.accept_ra_rtr_pref=0
```

Wenn die Einträge nicht vorhanden sind oder deren Werte nicht auf Null gesetzt sind, fügen Sie die Einträge hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

- 4 Speichern Sie alle von Ihnen vorgenommenen Änderungen und schließen Sie die Datei.

Verweigern von IPv6-Routerpräfixinformationen

Stellen Sie sicher, dass die Hostmaschinen der VMware-Appliance IPv6-Routerpräfixinformationen verweigern, es sei denn, sie sind für den Systembetrieb erforderlich.

Die `accept_ra_pinfo`-Einstellung steuert, ob das System Präfixinformationen aus dem Router akzeptiert. Wenn Adressen statisch zugewiesen werden, ist es nicht erforderlich, Routerpräfixinformationen zu empfangen.

Verfahren

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_pinfo | grep "default|all"` auf den Hostmaschinen der VMware-Appliance aus, um sicherzustellen, dass sie IPv6-Routerpräfixinformationen verweigern.

Wenn die Hostmaschinen für die Verweigerung der IPv6-Routerankündigungen konfiguriert sind, gibt dieser Befehl Folgendes zurück.

```
/proc/sys/net/ipv6/conf/all/accept_ra_pinfo:0
/proc/sys/net/ipv6/conf/default/accept_ra_pinfo:0
```

Wenn die Hostmaschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Wenn Sie Hostmaschinen für die Verweigerung von IPv6-Routerpräfixinformationen konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
- 3 Überprüfen Sie die folgenden Einträge.

```
net.ipv6.conf.all.accept_ra_pinfo=0
net.ipv6.conf.default.accept_ra_pinfo=0
```

Wenn die Einträge nicht vorhanden sind oder deren Werte nicht auf Null gesetzt sind, fügen Sie die Einträge hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

- 4 Speichern Sie die Änderungen und schließen Sie die Datei.

Verweigern der Hop-Limit-Einstellungen bei IPv6-Routerankündigungen

Stellen Sie sicher, dass die Hostmaschinen der VMware-Appliance Hop-Limit-Einstellungen der IPv6-Router verweigern, es sei denn, sie sind erforderlich.

Die `accept_ra_defrtr`-Einstellung steuert, ob das System Hop-Limit-Einstellungen aus einer Routerankündigung akzeptiert. Durch das Festlegen auf Null wird vorgebeugt, dass ein Router Ihr standardmäßiges IPv6-Hop-Limit für ausgehende Pakete ändert.

Verfahren

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_defrtr | egrep "default|all"` auf den Hostmaschinen der VMware-Appliance aus, um sicherzustellen, dass sie Hop-Limit-Einstellungen der IPv6-Router verweigern.

Wenn die Hostmaschinen für die Verweigerung von Hop-Limit-Einstellungen der IPv6-Router konfiguriert sind, gibt dieser Befehl Werte von 0 zurück.

```
/proc/sys/net/ipv6/conf/all/accept_ra_defrtr:0
/proc/sys/net/ipv6/conf/default/accept_ra_defrtr:0
```

Wenn die Hostmaschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Wenn Sie eine Hostmaschine für die Verweigerung der Hop-Limit-Einstellungen von IPv6-Routern konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
- 3 Überprüfen Sie die folgenden Einträge.

```
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.default.autoconf=0
```

Wenn die Einträge nicht vorhanden sind oder deren Werte nicht auf Null gesetzt sind, fügen Sie die Einträge hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

- 4 Speichern Sie alle von Ihnen vorgenommenen Änderungen und schließen Sie die Datei.

Verweigern der Autoconf-Einstellungen von IPv6-Routerankündigungen

Stellen Sie sicher, dass die Hostmaschinen der VMware-Appliance Autoconf-Einstellungen der IPv6-Router verweigern, sofern nicht erforderlich.

Die `autoconf`-Einstellung steuert, ob Routerankündigungen das Zuweisen einer globalen Unicast-Adresse zu einer Schnittstelle durch das System verursachen können.

Verfahren

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv6/conf/*/autoconf | egrep "default|all"` auf den Hostmaschinen der VMware-Appliance aus, um sicherzustellen, dass sie die Autoconf-Einstellungen der IPv6-Router verweigern.

Wenn die Hostmaschinen für die Verweigerung der Autoconf-Einstellungen von IPv6-Router konfiguriert sind, gibt dieser Befehl Werte von 0 zurück.

```
/proc/sys/net/ipv6/conf/all/autoconf:0
/proc/sys/net/ipv6/conf/default/autoconf:0
```

Wenn die Hostmaschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Wenn Sie eine Hostmaschine für die Verweigerung der Autoconf-Einstellungen von IPv6-Router konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.

3 Überprüfen Sie die folgenden Einträge.

```
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.default.autoconf=0
```

Wenn die Einträge nicht vorhanden sind oder deren Werte nicht auf Null gesetzt sind, fügen Sie die Einträge hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

4 Speichern Sie alle von Ihnen vorgenommenen Änderungen und schließen Sie die Datei.

Verweigern von IPv6-Nachbaranfragen

Stellen Sie sicher, dass die Hostmaschinen der VMware-Appliance IPv6-Nachbaranfragen verweigert, es sei denn, sie sind erforderlich.

Die `dad_transmits`-Einstellung legt fest, wie viele Nachbaranfragen pro Adresse (global und verbindungslokal) beim Anzeigen einer Schnittstelle gesendet werden, um sicherzustellen, dass die gewünschte Adresse im Netzwerk eindeutig ist.

Verfahren

- 1 Führen Sie den Befehl `# grep [01] /proc/sys/net/ipv6/conf/*/dad_transmits | grep "default|all"` auf den Hostmaschinen der VMware-Appliance aus, um zu bestätigen, dass sie IPv6-Nachbaranfragen verweigern.

Wenn die Hostmaschinen für die Verweigerung von IPv6-Nachbaranfragen konfiguriert sind, gibt dieser Befehl Werte von 0 zurück.

```
/proc/sys/net/ipv6/conf/all/dad_transmits:0
/proc/sys/net/ipv6/conf/default/dad_transmits:0
```

Wenn die Hostmaschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Wenn Sie eine Hostmaschine für die Verweigerung von IPv6-Nachbaranfragen konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
- 3 Überprüfen Sie die folgenden Einträge.

```
net.ipv6.conf.all.dad_transmits=0
net.ipv6.conf.default.dad_transmits=0
```

Wenn die Einträge nicht vorhanden sind oder deren Werte nicht auf Null gesetzt sind, fügen Sie die Einträge hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

- 4 Speichern Sie alle von Ihnen vorgenommenen Änderungen und schließen Sie die Datei.

Einschränken der maximalen Anzahl der IPv6-Adressen

Stellen Sie sicher, dass die Einstellungen für die maximale Anzahl der IPv6-Adressen für die Hostmaschinen Ihrer VMware-Appliances auf eine für den Betrieb des Systems notwendige Mindestanzahl festgelegt sind.

Die Einstellung für die maximale Anzahl der Adressen legt fest, wie viele IPv6-Adressen auf jeder Schnittstelle zur Verfügung stehen. Der Standardwert lautet 16, aber Sie sollten genau die Anzahl der statisch konfigurierten globalen Adressen festlegen, die für Ihr System erforderlich ist.

Verfahren

- 1 Führen Sie den `# grep [1] /proc/sys/net/ipv6/conf/*/max_addresses | egrep "default|all"`-Befehl auf den Hostmaschinen der VMware-Appliances aus, um sicherzustellen, dass die maximale Anzahl der IPv6-Adressen entsprechend eingeschränkt ist.

Wenn die Hostmaschinen zum Einschränken der maximalen Anzahl der IPv6-Adressen konfiguriert sind, gibt dieser Befehl die Werte 1 zurück.

```
/proc/sys/net/ipv6/conf/all/max_addresses:1
/proc/sys/net/ipv6/conf/default/max_addresses:1
```

Wenn die Hostmaschinen ordnungsgemäß konfiguriert sind, ist keine weitere Aktion erforderlich.

- 2 Wenn Sie die maximale Anzahl der IPv6-Adressen auf Hostmaschinen konfigurieren müssen, öffnen Sie die Datei `/etc/sysctl.conf` in einem Texteditor.
- 3 Überprüfen Sie die folgenden Einträge.

```
net.ipv6.conf.all.max_addresses=1
net.ipv6.conf.default.max_addresses=1
```

Wenn die Einträge nicht vorhanden oder deren Werte nicht auf 1 gesetzt sind, fügen Sie die Einträge hinzu oder aktualisieren Sie die vorhandenen Einträge entsprechend.

- 4 Speichern Sie alle von Ihnen vorgenommenen Änderungen und schließen Sie die Datei.

Konfigurieren von Netzwerkeinstellungen für den Infrastructure as a Service-Host

Konfigurieren Sie als Best Practice im Hinblick auf die Sicherheit die Einstellungen für die Netzwerkkommunikation auf der Hostmaschine der VMware-Infrastructure as a Service (IaaS)-Komponente gemäß den Anforderungen und Richtlinien von VMware.

Konfigurieren Sie die Netzwerkkonfiguration der Infrastructure as a Service (IaaS)-Hostmaschine, um die vollständigen vRealize Automation-Funktionen mit der entsprechenden Sicherheit zu unterstützen.

Siehe [Sichern der Infrastructure as a Service-Komponente](#).

Konfigurieren von Ports und Protokollen

Aus Sicherheitsgründen wird empfohlen, Ports und Protokolle für alle vRealize Automation-Appliances und -Komponenten gemäß den VMware-Richtlinien zu konfigurieren.

Konfigurieren Sie eingehende und ausgehende Ports für vRealize Automation-Komponenten gemäß den Anforderungen für kritische Systemkomponenten auf Produktionsebene. Deaktivieren Sie alle nicht benötigten Ports und Protokolle. Siehe *vRealize Automation-Referenzarchitektur* in der [Dokumentation zu VMware vRealize Automation](#).

Tool „Ports und Protokolle“

Mit dem Tool „Ports und Protokolle“ können Sie Portinformationen für zahlreiche VMware-Produkte auf einem einzelnen Dashboard anzeigen. Sie können ausgewählte Daten auch aus dem Tool für den Offline-Zugriff exportieren. Das Tool „Ports und Protokolle“ unterstützt aktuell:

- vSphere
- vSAN
- NSX for vSphere
- vRealize Network Insight
- vRealize Operations Manager
- vRealize Automation

Das Tool steht unter <https://ports.vmware.com/> zur Verfügung.

Für Benutzer erforderliche Ports

Aus Sicherheitsgründen wird die Konfiguration der vRealize Automation-Benutzerports gemäß den VMware-Richtlinien empfohlen.

Legen Sie erforderliche Ports nur über ein sicheres Netzwerk offen.

SERVER	PORTS
vRealize Automation-Appliance	443, 8443

Für Administrator erforderliche Ports

Konfigurieren Sie als Best Practice im Hinblick auf die Sicherheit vRealize Automation-Administratorports gemäß den VMware-Richtlinien.

Legen Sie erforderliche Ports nur über ein sicheres Netzwerk offen.

SERVER	PORTS
vRealize Application Services-Server	5480

vRealize Automation Appliance-Ports

Aus Sicherheitsgründen wird die Konfiguration von eingehenden und ausgehenden Ports für die vRealize Automation-Appliance gemäß den VMware-Empfehlungen empfohlen.

Eingehende Ports

Konfigurieren Sie die für die vRealize Automation-Appliance erforderliche Mindestanzahl an eingehenden Ports. Konfigurieren Sie optionale Ports, wenn diese für die Systemkonfiguration erforderlich sind.

Tabelle 8-1. Erforderliche Mindestanzahl an eingehenden Ports

PORT	PROTOKOLL	ANMERKUNGEN
443	TCP	Zugriff auf die vRealize Automation-Konsole und API-Aufrufe.
8443	TCP	VMware Remote Console-Proxy.
5480	TCP	Zugriff auf die Verwaltungsschnittstelle der vRealize Automation-Appliance.
5488, 5489	TCP	Intern. Von der vRealize Automation-Appliance für Updates verwendet.
5672	TCP	RabbitMQ-Messaging. Hinweis Wenn Sie vRealize Automation-Appliance-Instanzen clustern, müssen Sie möglicherweise die geöffneten Ports 4369 und 25672 konfigurieren.
40002	TCP	Für den vIDM-Dienst erforderlich. Beim Hinzufügen in einer HA-Konfiguration ist der gesamte externe Datenverkehr mit Ausnahme des Datenverkehrs von anderen vRealize Automation-Appliance-Knoten durch eine Firewall geschützt.

Konfigurieren Sie bei Bedarf optionale eingehende Ports.

Tabelle 8-2. Optionale eingehende Ports

PORT	PROTOKOLL	ANMERKUNGEN
22	TCP	(Optional) SSH. Deaktivieren Sie in einer Produktionsumgebung die SSH-Dienstüberwachung an Port 22 und schließen Sie Port 22.
80	TCP	(Optional) Umleitung an 443.

Ausgehende Ports

Konfigurieren Sie die erforderlichen ausgehenden Ports.

Tabelle 8-3. Erforderliche Mindestanzahl an ausgehenden Ports

PORT	PROTOKOLL	ANMERKUNGEN
25, 587	TCP, UDP	SMTP für das Senden von ausgehenden Benachrichtigungs-E-Mails.
53	TCP, UDP	DNS.
67, 68, 546, 547	TCP, UDP	DHCP.
110, 995	TCP, UDP	POP für das Empfangen von eingehenden Benachrichtigungs-E-Mails.
143, 993	TCP, UDP	IMAP für das Empfangen von eingehenden Benachrichtigungs-E-Mails.
443	TCP	Infrastructure as a Service-Manager Service über HTTPS.

Konfigurieren Sie bei Bedarf optionale ausgehende Ports.

Tabelle 8-4. Optionale ausgehende Ports

PORT	PROTOKOLL	ANMERKUNGEN
80	TCP	(Optional) Für das Abrufen von Softwareaktualisierungen. Sie können Aktualisierungen separat herunterladen und anwenden.
123	TCP, UDP	(Optional) Für das direkte Herstellen der Verbindung zu NTP anstatt der Verwendung von Hostzeit.

Tool „Ports und Protokolle“

Mit dem Tool „Ports und Protokolle“ können Sie Portinformationen für zahlreiche VMware-Produkte auf einem einzelnen Dashboard anzeigen. Sie können ausgewählte Daten auch aus dem Tool für den Offline-Zugriff exportieren. Das Tool „Ports und Protokolle“ unterstützt aktuell:

- vSphere
- vSAN
- NSX for vSphere
- vRealize Network Insight
- vRealize Operations Manager
- vRealize Automation

Die Tools sind unter <https://ports.vmware.com/> verfügbar.

Infrastructure as a Service-Ports

Aus Sicherheitsgründen wird die Konfiguration der eingehenden und ausgehenden Ports für Infrastructure as a Service (IaaS)-Komponenten gemäß den VMware-Richtlinien empfohlen.

Eingehende Ports

Konfigurieren Sie die erforderliche Mindestanzahl an eingehenden Ports für die IaaS-Komponenten.

Tabelle 8-5. Erforderliche Mindestanzahl an eingehenden Ports

KOMPONENTE	PORT	PROTOKOLL	ANMERKUNGEN
Manager Service	443	TCP	Kommunikation mit IaaS-Komponenten und vRealize Automation Appliance über HTTPS. Bei allen von Proxy-Agents verwalteten Virtualisierungshosts muss TCP-Port 443 für eingehenden Datenverkehr geöffnet sein.

Ausgehende Ports

Konfigurieren Sie die erforderliche Mindestanzahl an ausgehenden Ports für die IaaS-Komponenten.

Tabelle 8-6. Erforderliche Mindestanzahl an ausgehenden Ports

KOMPONENTE	PORT	PROTOKOLL	ANMERKUNGEN
Alle	53	TCP, UDP	DNS.
Alle		TCP, UDP	DHCP.

Tabelle 8-6. Erforderliche Mindestanzahl an ausgehenden Ports (Fortsetzung)

KOMPONENTE	PORT	PROTOKOLL	ANMERKUNGEN
Manager Service	443	TCP	Kommunikation mit vRealize Automation Appliance über HTTPS.
Website	443	TCP	Kommunikation mit Manager Service über HTTPS.
Distributed Execution Manager	443	TCP	Kommunikation mit Manager Service über HTTPS.
Proxy-Agents	443	TCP	Kommunikation mit Manager Service und Virtualisierungshosts über HTTPS.
Gast-Agent	443	TCP	Kommunikation mit Manager Service über HTTPS.
Manager Service, Website	1433	TCP	MSSQL.

Konfigurieren Sie optionale ausgehende Ports, falls erforderlich.

Tabelle 8-7. Optionale ausgehende Ports

KOMPONENTE	PORT	PROTOKOLL	ANMERKUNGEN
Alle	123	TCP, UDP	NTP ist optional.

Überwachung und Protokollierung

9

Richten Sie als Best Practice im Hinblick auf die Sicherheit Überwachung und Protokollierung auf dem vRealize Automation-System gemäß den Empfehlungen für VMware ein.

Remoteprotokollierung auf einem zentralen Protokollhost bietet einen sicheren Speicher für Protokolldateien. Mit dem Erfassen von Protokolldateien auf einem zentralen Host können Sie die Umgebung mit einem einzigen Tool überwachen. Darüber hinaus können Sie eine Aggregatanalyse durchführen und nach Hinweisen auf Bedrohungen wie koordinierte Angriffe auf mehrere Entitäten innerhalb der Infrastruktur suchen. Die Protokollierung auf einem sicheren, zentralisierten Protokollserver kann das Verhindern von Protokollmanipulation unterstützen und bietet außerdem eine langfristige Prüfungsaufzeichnung.

Sicherstellen, dass der Remote-Protokollierungsserver sicher ist

Nachdem Angreifer die Sicherheit des Hostcomputers verletzt haben, versuchen diese oft, nach Protokolldateien zu suchen und diese zu manipulieren, um ihre Spuren zu verdecken und die Kontrolle zu behalten, ohne entdeckt zu werden. Durch das Sichern des Remote-Protokollierungsservers wird entsprechend die Verhinderung der Manipulation von Protokollen unterstützt.

Verwenden eines autorisierten NTP-Servers

Stellen Sie sicher, dass alle Hostmaschinen dieselbe relative Zeitquelle, einschließlich des relevanten Lokalisierungsoffsets, verwenden und dass Sie die relative Zeitquelle auf einen vereinbarten Zeitstandard wie z. B. die koordinierte Weltzeit (UTC) korrelieren können. Mit einem disziplinierten Herangehen an Zeitquellen können Sie schnell Aktionen eines Eindringlings nachverfolgen und korrelieren, wenn Sie die relevanten Protokolldateien überprüfen. Bei falschen Zeiteinstellungen kann es schwierig werden, Protokolldateien zur Erkennung von Angriffen zu untersuchen und zu korrelieren. Dies kann zu ungenauen Ergebnissen bei der Überprüfung führen.

Verwenden Sie mindestens drei NTP-Server von externen Zeitquellen oder konfigurieren Sie einige lokale NTP-Server auf einem vertrauenswürdigen Netzwerk, die wiederum deren Uhrzeit von mindestens drei externen Zeitquellen erhalten.