

Handleiding Beveiligde configuratie

24 oktober 2019

vRealize Automation 7.6



vmware®

U vindt de recentste technische documentatie op de website van VMware:

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

Als u opmerkingen over deze documentatie heeft, kunt u uw feedback sturen naar:

docfeedback@vmware.com

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

VMware Nederland B.V.
Key Office Papendorp
3e verdieping
Orteliuslaan 850
Utrecht
Nederland
Tel: +31 (0) 30-2849500
Fax: +31 (0) 30- 2849501
www.vmware.com/nl

Copyright © 2015-2019 VMware, Inc. Alle rechten voorbehouden. [Informatie over copyright en handelsmerken.](#)

Inhoud

1	Beveiligde configuratie	5
2	Overzicht vRealize Automation-baselinebeveiliging	6
3	De integriteit van installatiemedia controleren	8
4	Hardening van software-infrastructuur van VMware-systeem	9
	De VMware vSphere ® -omgeving harden	9
	De Infrastructure as a Service-host harden	9
	Microsoft SQL Server harden	10
	Microsoft .NET harden	10
	Hardening van Internet Information Services (IIS)	10
5	Geïnstalleerde software controleren	12
6	VMware Veiligheidsadviezen en patches	13
7	Beveiligde configuratie	14
	De vRealize Automation-toepassing beveiligen	14
	Het hoofdwachtwoord wijzigen	14
	Hash en complexiteit van rootwachtwoord controleren	15
	Rootwachtwoordgeschiedenis controleren	15
	Verlopen van wachtwoorden beheren	16
	Beheren van Secure Shell- en beheerdersaccounts	17
	De Virtual Appliance Management Interface-gebruiker wijzigen	21
	Boot Loader-verificatie instellen	22
	NTP configureren	22
	TLS voor gegevens in overdracht configureren voor de vRealize Automation-toepassing	23
	De beveiliging van Data-at-Rest controleren	32
	vRealize Automation-toepassingsbronnen configureren	33
	Configuratie van consoleproxy aanpassen	35
	Serverresponseheaders configureren	38
	Sessie-time-out vRealize Automation-toepassing instellen	39
	Niet-essentiële software beheren	39
	Het onderdeel Infrastructure as a Service beveiligen	44
	NTP configureren	44
	TLS voor Infrastructure as a Service Data-in-Transit configureren	44
	TLS-coderingssuites configureren	47

Beveiliging van hostserver controleren	48
Toepassingsbronnen beschermen	48
De Infrastructure as a Service-hostmachine beveiligen	49

8 Hostnetwerkbeveiliging configureren 51

Netwerkinstellingen configureren voor VMware-toepassingen	51
Toegang van gebruikers tot netwerkinterfaces voorkomen	51
Wachtrijgrootte TCP Backlog instellen	52
ICMPv4-echo's naar uitzendadres weigeren	52
IPv4-proxy ARP uitschakelen	53
IPv4 ICMP-omleidingsberichten weigeren	53
IPv6 ICMP-omleidingsberichten weigeren	54
IPv4-martian-pakketten opslaan in logboek	55
Omgekeerde padfiltering van IPv4 gebruiken	55
IPv4-forwarding weigeren	56
IPv6-forwarding weigeren	57
IPv4 TCP Syncookies gebruiken	57
IPv6-router-advertisements weigeren	58
IPv6-routeraanvragen weigeren	59
IPv6-routervoorkeuren in routeraanvragen weigeren	59
IPv6-routervoorvoegsels weigeren	60
Hop-limit-instellingen van IPv6-router-advertisement weigeren	61
Autoconf-instellingen voor IPv6-router-advertisement weigeren	61
IPv6-neighbor-aanvragen weigeren	62
Max. aantal IPv6-adressen beperken	63
Netwerkinstellingen voor de Infrastructure as a Service-host configureren	64
Poorten en protocollen configureren	64
Voor gebruikers verplichte poorten	64
Voor beheerders vereiste poorten	65

9 Audits en logboekregistratie 68

Beveiligde configuratie

Beveiligde configuratie helpt gebruikers bij het evalueren en optimaliseren van de beveiligde configuratie van vRealize Automation-implementaties.

In Beveiligde configuratie wordt de verificatie en configuratie van beveiligde implementaties voor typische vRealize Automation-omgevingen beschreven, en het biedt informatie en procedures aan de hand waarvan gebruikers geïnformeerde beslissingen kunnen nemen over een beveiligde configuratie.

Doelgroep

Deze informatie is bedoeld voor systeembeheerders van vRealize Automation en andere gebruikers die verantwoordelijk zijn voor het beheer en de configuratie van de systeembeveiliging.

Woordenlijst VMware Technical Publications

VMware Technical Publications biedt een woordenlijst met de termen die u mogelijk nog niet kent. Ga naar <http://www.vmware.com/support/pubs> voor een definitie van de termen die in de technische documentatie van VMware worden gebruikt.

Overzicht vRealize Automation-baselinebeveiliging

2

VMware bevat uitgebreide aanbevelingen voor het controleren en configureren van een veilige baseline voor uw vRealize Automation-systeem.

Gebruik de juiste tools en procedures van VMware voor het controleren en behouden van een veilige, harde baseline-configuratie voor uw vRealize Automation-systeem. Sommige vRealize Automation-onderdelen zijn geïnstalleerd in een geharde of gedeeltelijke geharde staat, maar u moet de configuratie van ieder onderdeel controleren en bekijken in het licht van VMware beveiligingsaanbevelingen, bedrijfsveiligheidsregels en bekende dreigingen.

vRealize Automation Beveiligingregels

De beveiligingsregels van vRealize Automation gaan uit van een holistisch beveiligde omgeving gebaseerd op systeem- en netwerkconfiguratie, organisationele beveiligingsregels en best practices op het gebied van veiligheid.

Ga bij het controleren en configureren van de hardening van een vRealize Automation-systeem uit van de volgende aanbevelingen van VMware.

- Veilige implementatie
- Beveiligde configuratie
- Netwerkbeveiliging

Om te zorgen dat uw systeem veilig gehard wordt, moet u de aanbevelingen van VMware en uw lokale veiligheidsregels in acht nemen, omdat deze van toepassing zijn op al deze conceptuele gebieden.

Systeemonderdelen

Om een geharde, veilige configuratie van uw vRealize Automation-systeem te realiseren, moet u alle onderdelen kennen en weten hoe ze samenwerken bij de ondersteuning van de systeemfuncties.

Denk aan de volgende onderdelen bij het plannen en implementeren van systeembeveiliging.

- vRealize Automation-toepassing
- IaaS-onderdeel

Als u meer wilt weten over vRealize Automation en de manier waarop de onderdelen samenwerken, raadpleegt u *Basisprincipes en concepten* in het VMware vRealize Automation-documentatiecentrum. Zie *Referentie-architectuur* voor meer informatie over typische vRealize Automation-implementaties en -architectuur. U vindt meer gerelateerde documentatie in de [documentatie voor VMware vRealize Automation](#).

De integriteit van installatiemedia controleren

3

Gebruikers moeten altijd de integriteit van de installatiemedia controleren voordat ze een VMware-product installeren.

Controleer altijd de SHA1 hash of patch nadat u een ISO offline bundel downloadt om de integriteit en originaliteit van de gedownloade bestanden te waarborgen. Als u fysieke media ontvangt van VMware waarvan het veiligheidszegel verbroken is, retourneer de software dan aan VMware voor vervanging.

Gebruik nadat u de software gedownload hebt de totaalwaarde MD5/SHA1 om de integriteit van de download te controleren. Vergelijk de MD5/SHA1 hash-uitvoer met de waarde die vermeld is op de website van VMware. SHA1 of MD5 hash moet overeenkomen.

Voor meer informatie over het controleren van de integriteit van installatiemedia, zie <http://kb.vmware.com/kb/1537>.

Hardening van software-infrastructuur van VMware-systeem

4

Beoordeel de geïmplementeerde software-infrastructuur die uw VMware-systeem ondersteunt en controleer of hij voldoet aan de VMware-richtlijnen voor hardening, als onderdeel van uw verhardingsproces.

Voordat u uw VMware-systeem verhardt, dient u beveiligingsgebreken te beoordelen en op te lossen in uw ondersteunende software-infrastructuur om een volledig geharde en beveiligde omgeving te maken. Elementen van de software-infrastructuur die u moet overwegen, zijn onder andere onderdelen van het besturingssysteem, ondersteunende software en database-software. Los beveiligingsproblemen in deze en andere onderdelen op met behulp van de aanbevelingen van de fabrikant en andere relevante beveiligingsprotocollen.

Dit hoofdstuk omvat de volgende onderwerpen:

- [De VMware vSphere® -omgeving harden](#)
- [De Infrastructure as a Service-host harden](#)
- [Microsoft SQL Server harden](#)
- [Microsoft .NET harden](#)
- [Hardening van Internet Information Services \(IIS\)](#)

De VMware vSphere® -omgeving harden

Beoordeel de VMware vSphere® -omgeving en controleer of het juiste niveau van vSphere-hardening wordt afgedwongen en gehandhaafd.

Voor meer hulp over hardening, zie <http://www.vmware.com/security/hardening-guides.html>.

Als onderdeel van een uitgebreid geharde omgeving, moet de VMware vSphere® -infrastructuur voldoen aan beveiligingsrichtlijnen zoals opgesteld door VMware.

De Infrastructure as a Service-host harden

Verifieer of uw Infrastructure as a Service Microsoft Windows-hostmachine is gehard volgens de richtlijnen van VMware.

Bekijk de aanbevelingen die worden gegeven in de aanbevolen richtlijnen van Microsoft Windows voor hardening en beveiliging en zorg dat uw Windows Server-host voldoende gehard is. Het niet opvolgen van de aanbevelingen voor hardening kan leiden tot blootstelling aan bekende beveiligingsrisico's van Windows-versies.

Zie de [vRealize Automation-ondersteuningsmatrix](#) om te controleren of uw versie wordt ondersteund.

Neem contact op met uw Microsoft-leverancier over de juiste hulp voor het harden van Microsoft-producten.

Microsoft SQL Server harden

Verifieer of de Microsoft SQL-serverdatabase voldoet aan de richtlijnen die zijn opgesteld door Microsoft en VMware.

Bekijk de aanbevelingen die worden gegeven in de richtlijnen van Microsoft SQL-server voor hardening en beveiliging. Bekijk ook alle beveiligingsbulletins van Microsoft over de geïnstalleerde versie van Microsoft SQL Server. Het niet opvolgen van de aanbevelingen voor hardening kan leiden tot blootstelling aan bekende beveiligingsrisico's van Microsoft SQL Server-versies.

Zie de [vRealize Automation-ondersteuningsmatrix](#) om te controleren of uw versie van Microsoft SQL Server wordt ondersteund.

Neem contact op met uw Microsoft-leverancier voor richtlijnen voor het harden van Microsoft-producten.

Microsoft .NET harden

Als onderdeel van een uitgebreid geharde omgeving, moet Microsoft .NET voldoen aan beveiligingsrichtlijnen zoals deze zijn opgesteld door Microsoft en VMware.

Bekijk de aanbevelingen die worden gegeven in de passende .NET-hardening en aanbevolen beveiligingsrichtlijnen. Bekijk ook alle beveiligingsbulletins van Microsoft over de versie van Microsoft SQL Server die u gebruikt. Het niet opvolgen van de aanbevelingen voor hardening kan leiden tot blootstelling aan bekende beveiligingsrisico's van onbeveiligde Microsoft.NET-onderdelen.

Zie de [vRealize Automation-ondersteuningsmatrix](#) om te controleren of uw versie van Microsoft.NET wordt ondersteund.

Neem contact op met uw Microsoft-leverancier voor richtlijnen voor het harden van Microsoft-producten.

Hardening van Internet Information Services (IIS)

Verifieer of uw Microsoft Internet Information Services (IIS) voldoet aan alle beveiligingsrichtlijnen van Microsoft en VMware.

Bekijk de aanbevelingen die worden gegeven in de aanbevolen richtlijnen voor passende Microsoft IIS-hardening en beveiliging. Bekijk ook alle beveiligingsbulletins van Microsoft over de versie van IIS die u gebruikt. Het niet opvolgen van de aanbevelingen voor hardening kan leiden tot blootstelling aan bekende beveiligingsrisico's.

Zie de [vRealize Automation-ondersteuningsmatrix](#) om te controleren of uw versie wordt ondersteund.

Neem contact op met uw Microsoft-leverancier voor richtlijnen voor het harden van Microsoft-producten.

Geïnstalleerde software controleren

5

Omdat kwetsbaarheden in software van derden en ongebruikte software het risico op onbevoegde toegang tot het systeem en verstoring van beschikbaarheid verhogen, is het belangrijk alle software die geïnstalleerd is op VMware-hostmachines te controleren en het gebruik ervan te evalueren.

Installeer geen software die niet nodig is voor het veilige gebruik van het systeem op de VMware-hostmachines. Verwijder ongebruikte of externe software.

Inventarisatie niet-ondersteunde software-installaties

Controleer uw VMware-implementatie en inventaris van geïnstalleerde producten om te controleren of er geen externe, niet-ondersteunde software geïnstalleerd is.

Zie voor meer informatie over de ondersteuningsregels van producten van derde partijen het VMware-artikel over ondersteuning op <https://www.vmware.com/support/policies/thirdparty.html>.

Software van derden controleren

De installatie van software van derden die niet is getest en gecontroleerd, wordt ondersteund noch aanbevolen door VMware. Onveilige, niet-geverifieerde software van derden zonder patches die op VMware-hostmachines is geïnstalleerd, brengt het risico op onbevoegde toegang tot het systeem en verstoring van beschikbaarheid met zich mee. Als u niet-ondersteunde software van derden moet gebruiken, vraag dan de externe verkoper om advies over veilige configuratie en patching-vereisten.

VMware Veiligheidsadviezen en patches

6

Om uw systeem maximaal te beveiligen, volgt u de beveiligingsadviezen van VMware en past u alle relevante patches toe.

VMware geeft beveiligingsadviezen voor producten. Houd deze adviezen in de gaten om te zorgen dat uw product beveiligd is tegen bekende dreigingen.

Open de installatie-, patching- en upgradegeschiedenis van vRealize Automation en controleer of de gegeven beveiligingsadviezen van VMware gevolgd en uitgevoerd zijn.

Voor meer informatie over de huidige beveiligingsadviezen van VMware, zie <http://www.vmware.com/security/advisories/>.

Beveiligde configuratie

Controleer en bewerk de beveiligingsinstellingen voor vRealize Automation virtual appliances en het onderdeel Infrastructure as a Service voor uw systeemconfiguratie. Controleer en bewerk daarnaast de configuratie van andere onderdelen en toepassingen.

Onder het veilig configureren van een vRealize Automation-installatie valt het controleren van de configuratie van ieder onderdeel afzonderlijk en van de onderdelen gezamenlijk. Overweeg alle systeemonderdelen samen te configureren zodat u een redelijk goede baselinebeveiliging krijgt.

Dit hoofdstuk omvat de volgende onderwerpen:

- [De vRealize Automation-toepassing beveiligen](#)
- [Het onderdeel Infrastructure as a Service beveiligen](#)

De vRealize Automation-toepassing beveiligen

Controleer en bewerk de beveiligingsinstellingen voor de vRealize Automation-toepassing in de mate die vereist is voor uw systeemconfiguratie.

Configureer beveiligingsinstellingen voor uw virtual appliances en voor de besturingssystemen waarop deze worden uitgevoerd. Daarnaast moet u de configuratie van andere gerelateerde onderdelen en toepassingen instellen of controleren. In sommige gevallen moet u bestaande instellingen controleren, in andere gevallen moet u instellingen aanpassen of toevoegen om tot een juiste configuratie te komen.

Het hoofdwachtwoord wijzigen

U kunt het hoofdwachtwoord wijzigen voor de vRealize Automation-toepassing.

Procedure

- 1 Meld u aan bij de vRealize Automation-toepassingsbeheerinterface als root.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Klik op het tabblad **Beheer**.
- 3 Klik op het submenu **Beheer**.
- 4 Voer het huidige wachtwoord in in het tekstvak **Huidig wachtwoord van beheerder**.
- 5 Voer het nieuwe wachtwoord in in het tekstvak **Nieuw wachtwoord van beheerder**.
- 6 Voer het nieuwe wachtwoord in in het tekstvak **Nieuw wachtwoord van beheerder opnieuw typen**.

7 Klik op **Instellingen opslaan**.

Hash en complexiteit van rootwachtwoord controleren

Controleer of het hoofdwachtwoord voldoet aan de bedrijfsvereisten van uw organisatie voor de complexiteit van wachtwoorden.

Het is verplicht de complexiteit van het rootwachtwoord te controleren als de rootgebruiker de pam_cracklib-module voor controle van wachtwoordcomplexiteit die toegepast wordt op gebruikersaccounts omzeilt.

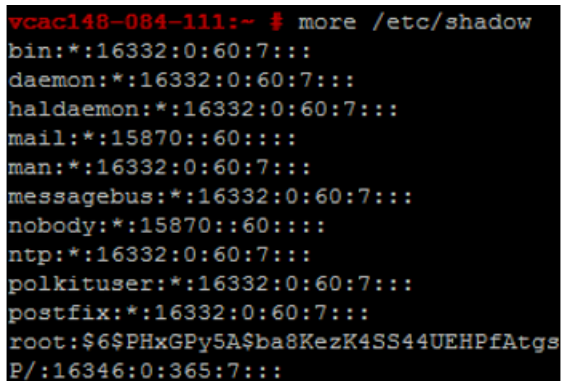
Het accountwachtwoord moet beginnen met \$6\$, wat staat voor een sha512 hash. Dit is de standaard-hash voor alle geharde toepassingen.

Procedure

- 1 Om de hash van het rootwachtwoord te controleren, meldt u zich aan als root en voert u de opdracht `# more /etc/shadow` uit.

De hash-informatie wordt weergegeven.

Figuur 7-1. Resultaten wachtwoord-hash



```
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 Als het rootwachtwoord geen sha512 hash bevat, voer dan de opdracht `passwd` uit om dit te veranderen.

Alle beveiligde toepassingen schakelen `enforce_for_root` in voor de module `pw_history`, die u vindt in het bestand `etc/pam.d/common-password`. Het systeem onthoudt standaard de laatste vijf wachtwoorden. Oude wachtwoorden worden voor iedere gebruiker opgeslagen in het bestand `/etc/securetty/passwd`.

Rootwachtwoordgeschiedenis controleren

Controleer of de wachtwoordgeschiedenis is uitgevoerd voor het rootaccount.

Met alle beveiligde toepassingen wordt `enforce_for_root` ingeschakeld voor de module `pw_history`, die u vindt in het bestand `etc/pam.d/common-password`. Het systeem onthoudt standaard de laatste vijf wachtwoorden. Oude wachtwoorden worden voor iedere gebruiker opgeslagen in het bestand `/etc/securetty/passwd`.

Procedure

- 1 Voer de volgende opdracht uit:

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

- 2 Controleer of `enforce_for_root` wordt weergegeven in de gevonden resultaten.

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

Verlopen van wachtwoorden beheren

Configureer de verlooptdata van alle accountwachtwoorden in overeenstemming met het veiligheidsbeleid van uw organisatie.

Standaard gebruiken alle geharde virtuele VMware-accounts een vervalttermijn van 60 dagen voor het wachtwoord. Op de meeste geharde toepassingen is het rootaccount ingesteld op een vervalttermijn van 365 dagen voor het wachtwoord. Wij raden u aan te verifiëren of de vervaldatum op alle accounts overeenkomt met zowel de standaard veiligheids- als bewerkingseisen.

Als het rootwachtwoord verloopt, kunt u het niet opnieuw in gebruik nemen. U moet een site-specifiek beleid implementeren om te voorkomen dat beheer- en rootwachtwoorden verlopen.

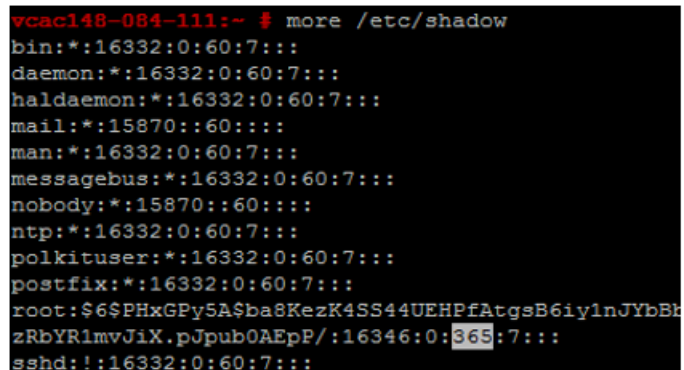
Procedure

- 1 Meld u aan bij uw machines met virtual appliances als root en voer de volgende opdracht uit om het verlopen van wachtwoorden op alle accounts te verifiëren.

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

Het verlopen van het wachtwoord staat in het vijfde veld (velden zijn gescheiden door komma's) van het schaduwbestand. Het vervallen van de root is ingesteld in dagen.

Figuur 7-2. Verlopen van wachtwoorden



```
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 Om het verlopen van het rootaccount te wijzigen, voert u een opdracht met de volgende vorm uit.

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


In deze opdracht staat 365 voor het aantal dagen tot de vervaldatum van het wachtwoord. Gebruik dezelfde opdracht om een gebruiker te wijzigen, waarbij u het specifieke account in de plaats van 'root' gebruikt en het aantal dagen vervangt waarbinnen een wachtwoord volgens standaarden van de organisatie moet worden vervangen.

Beheren van Secure Shell- en beheerdersaccounts

Voor externe verbindingen beschikken alle geharde appliances over het Secure Shell-protocol (SSH). Gebruik SSH alleen wanneer dit nodig is, en beheer het zo dat de systeemveiligheid behouden blijft.

SSH is een interactieve omgeving met een opdrachtregel die externe verbindingen ondersteunt naar VMware virtuele toepassingen. Standaard zijn voor SSH-toegang verificatiegegevens voor high-privileged gebruikersaccounts nodig. De SSH-activiteiten van de hoofdgebruiker slaan de op rollen gebaseerde toegangscontrole (RBAC) en auditcontrole van de virtuele toepassingen meestal over.

Schakel als best practice SSH uit in een productie-omgeving, en activeer het alleen om problemen op te lossen die u niet op andere wijze kunt oplossen. Laat het alleen ingeschakeld indien nodig voor een specifiek doel en in overeenstemming met de veiligheidsregels van uw organisatie. SSH wordt standaard uitgeschakeld op de vRealize Automation-toepassing. Afhankelijk van uw configuratie van vSphere, kan het zijn dat u SSH kan in- of uitschakelen als u gebruik maakt van uw Open Virtualization Format-sjabloon (OVF).

Voor een eenvoudige test om te controleren of SSH is ingeschakeld op een machine, kunt u een verbinding proberen te openen met behulp van SSH. Als de verbinding geopend wordt en er om verificatiegegevens gevraagd wordt, is SSH ingeschakeld en beschikbaar voor verbindingen.

Hoofdgebruikersaccount Secure Shell

Omdat VMware toepassingen niet beschikken over vooraf geconfigureerde gebruikersaccounts, kan het hoofdaccount SSH gebruiken om direct standaard aan te melden. Schakel SSH zo snel mogelijk met het hoofdaccount uit.

Om de standaard voor onverwervelijkheid na te leven, is de SSH-server op alle geharde toepassingen geconfigureerd met de AllowGroups-wielinvoer voor het beperken van SSH-toegang tot het secundaire groepswiel. Voor scheiding van verplichtingen kunt u de AllowGroups-wielinvoer in het bestand `/etc/ssh/sshd_config` aanpassen naar het gebruik van een andere groep, zoals `sshd`.

De wielgroep heeft de module `pam_wheel` voor superuser-toegang ingeschakeld, zodat leden van de wielgroep `su-root` kunnen uitvoeren waar het hoofdwachtwoord benodigd is. Door groepscheiding kunnen gebruikers SSH gebruiken om de toepassing te openen, maar geen `su` naar de root uitvoeren. Verwijder of verander geen andere invoer in het veld AllowGroups, dat zorgt voor de juiste functionaliteit van de toepassing. Als u een verandering hebt uitgevoerd, moet u de SSH daemon opnieuw starten door de volgende opdracht uit te voeren: `# service sshd restart`.

Secure Shell in- of uitschakelen op vRealize Automation-toepassingen

Schakel Secure Shell (SSH) op de vRealize Automation-toepassing uitsluitend in voor probleemoplossing. Schakel SSH uit op deze onderdelen tijdens de normale productie.

U kunt SSH op de vRealize Automation-toepassing in- of uitschakelen door de beheerinterface van de vRealize Automation-toepassing te gebruiken.

Procedure

- 1 Meld u aan bij de vRealize Automation-toepassingsbeheerinterface als root.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Klik op het tabblad **Beheer**.
- 3 Klik op het submenu **Beheer**.
- 4 Selecteer het keuzevakje **SSH-service inschakelen** om SSH in te schakelen en deselecteer het om SSH uit te schakelen.
- 5 Klik op **Instellingen opslaan** om uw wijzigingen op te slaan.

Lokale beheerdersaccount voor Secure Shell maken

De aanbevolen beveiligingsprocedure is lokale beheerdersaccounts voor Secure Shell (SSH) te maken en te configureren op de hostmachines van uw virtual appliances. Daarnaast moet u toegang tot de SSH-hoofdmap uitschakelen nadat u de accounts hebt gemaakt.

Maak lokale beheerdersaccounts voor SSH, leden van de secundaire 'wheel-groep' of beide. Voordat u toegang tot de hoofdmap uitschakelt, moet u testen of geautoriseerde beheerders toegang hebben tot SSH met AllowGroups, en of zij su naar de root kunnen uitvoeren via de wheel-groep.

Procedure

- 1 Meld u als root aan bij de virtual appliances en voer de volgende opdrachten met de bijbehorende gebruikersnaam.

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

Wheel is de groep zoals gespecificeerd in AllowGroups voor SSH-toegang. Gebruik `-G wheel,sshd` om meerdere secundaire groepen toe te voegen.

- 2 Schakel naar de gebruiker en geef een nieuw wachtwoord op om dit te controleren op complexiteit.

```
# su -gebruikersnaam
# gebruikersnaam@hostnaam:~>passwd
```

Als het wachtwoord de gewenste complexiteit heeft, wordt het wachtwoord bijgewerkt. Als het wachtwoord niet de gewenste complexiteit heeft, wordt het oorspronkelijke wachtwoord teruggezet en moet u de wachtwoordopdracht opnieuw uitvoeren.

- Als u rechtstreeks aanmelden bij SSH wilt verwijderen, moet u het bestand `/etc/ssh/sshd_config` aanpassen door `(#)PermitRootLogin yes` te vervangen door `PermitRootLogin no`.

U kunt ook SSH in de Virtual Appliance Management Interface (VAMI) inschakelen/uitschakelen door het selectievakje **Bij SSH aanmelden als beheerder ingeschakeld** op het tabblad **Beheer** in of uit te schakelen.

Wat nu te doen

Schakel rechtstreeks aanmelden als root uit. De verharde toepassingen staan rechtstreeks aanmelden als root via de console standaard toe. Als u beheerdersaccounts hebt gemaakt voor niet-afwijzing en deze hebt getest op su-root wheel-toegang, schakelt u rechtstreeks aanmelden als root uit door het bestand `/etc/security` als root te bewerken en de `tty1`-invoer te vervangen met `console`.

- Open het bestand `/etc/securetty` in een teksteditor.
- Zoek `tty1` en vervang dit door `console`.
- Sla het CSV-bestand op en sluit het.

Hardening van de Secure Shell-serverconfiguratie

Waar mogelijk hebben alle VMware-toepassingen een standaard geharde configuratie. Gebruikers kunnen controleren of hun configuratie voldoende gehard is door de server en de clientservice-instellingen in het gedeelte Globale opties van het configuratiebestand te onderzoeken.

Procedure

- Open het serverconfiguratiebestand `/etc/ssh/sshd_config` op de VMware-toepassing en controleer of de instellingen correct zijn.

Instelling	Status
Serverdaemonprotocol	Protocol 2
CBC-codes	aes256-ctr en aes128-ctr
TCP-forwarding	AllowTCPForwarding nee
Servergatewaypoorten	Clientgatewaypoorten nee
X11-forwarding	X11Forwarding nee
SSH-service	Gebruik het veld AllowGroups en specificeer een voor de groep toegestane toegang. Voeg de juiste leden toe aan deze groep.
GSSAPI-verificatie	GSSAPIAuthentication nee, indien niet gebruikt
Keberos-verificatie	KeberosAuthentication nee, indien niet gebruikt
Lokale variabelen (globale optie AcceptEnv)	Stel in op uitgeschakeld door uitcommentariëren of ingeschakeld voor <code>LC_*</code> of <code>LANG</code> -variabelen
Tunnelconfiguratie	PermitTunnel nee
Netwerksessies	MaxSessions 1

Instelling	Status
Gebruiker van concurrerende verbindingen	Stel in op 1 voor hoofdmap en elke andere gebruiker. Het bestand <code>/etc/security/limits.conf</code> moet ook worden geconfigureerd met dezelfde instelling.
Controleren van de strict-modus	Strict-modus ja
Scheiding van privileges	UsePrivilegeSeparation ja
rhosts RSA-verificatie	RhostsESAAuthentication nee
Compressie	Compressie vertraagd of Compressie nee
Berichtverificatiemodus	MACs hmac-sha1
Beperking van gebruikerstoegang	PermitUserEnvironment nee

2 Sla uw wijzigingen op en sluit het bestand.

Hardening van de Secure Shell-clientconfiguratie

Als onderdeel van het hardingsproces van uw systeem controleert u de harding van de SSH-client door de het configuratiebestand van de SSH-client op machines die virtual appliances hosten om zeker te zijn dat hij is geconfigureerd volgens de richtlijnen van VMware.

Procedure

- 1 Open het SSH-clientconfiguratiebestand `/etc/ssh/ssh_config` en controleer of de instellingen in het gedeelte globale opties correct zijn.

Instelling	Status
Clientprotocol	Protocol 2
Clientgatewaypoorten	Clientgatewaypoorten nee
GSSAPI-verificatie	GSSAPI-verificatie nee
Lokale variabelen (globale optie SendEnv)	Bied uitsluitend <code>LC_*</code> of <code>LANG</code> -variabelen
CBC-codes	uitsluitend aes256-ctr en aes128-ctr
Berichtverificatiecodes	Uitsluitend gebruikt in de vermelding MACs hmac-sha1

2 Sla uw wijzigingen op en sluit het bestand.

Rechten voor Secure Shell-sleutelbestanden controleren

Om de kans op een kwaadwillende aanval zo klein mogelijk te maken, moet u kritieke rechten voor SSH-sleutelbestanden op de hostmachines van uw virtual appliances behouden.

Na het configureren of bijwerken van uw SSH-configuratie moet u altijd controleren of de rechten van het volgende SSH-sleutelbestand niet gewijzigd zijn.

- De sleutelbestanden van de openbare host in `/etc/ssh/*key.pub/` zijn in eigendom van de rootgebruiker en hebben rechten ingesteld tot 0644 (`-rw-r--r--`).

- De sleutelbestanden van de privé-host in `/etc/ssh/*key` zijn in eigendom van de rootgebruiker en hebben rechten ingesteld tot 0600 (`-rw----`).

Rechten voor SSH-sleutelbestand controleren

Controleer of SSH-rechten van toepassing zijn op zowel openbare als persoonlijke sleutelbestanden.

Procedure

- 1 Controleer de openbare SSH-sleutelbestanden door de volgende opdracht uit te voeren: `ls -l /etc/ssh/*key.pub`
- 2 Controleer of de eigenaar root is, of de groepseigenaar root is en of voor de bestanden de rechten zijn ingesteld op 0644 (`-rw-r--r--`).
- 3 Los eventuele problemen op door de volgende opdrachten uit te voeren.


```
chown root /etc/ssh/*key.pub
chgrp root /etc/ssh/*key.pub
chmod 644 /etc/ssh/*key.pub
```
- 4 Controleer de persoonlijke SSH-sleutelbestanden door de volgende opdracht uit te voeren: `ls -l /etc/ssh/*key`
- 5 Controleer of de eigenaar root is, of de groepseigenaar root is en of voor de bestanden de rechten zijn ingesteld op 0600 (`-rw-----`). Los eventuele problemen op door de volgende opdrachten uit te voeren.


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

De Virtual Appliance Management Interface-gebruiker wijzigen

U kunt gebruikers in de Virtual Appliance Management Interface toevoegen en verwijderen om het juiste niveau van beveiliging te creëren.

Voor het rootgebruikersaccount van de Virtual Appliance Management Interface wordt PAM gebruikt voor verificatie. Hierdoor zijn de door PAM ingestelde opnameniveaus ook van toepassing. Als u de Virtual Appliance Management Interface niet juist hebt geïsoleerd, kan er een vergrendeling van het systeemrootaccount optreden als wordt getracht een beveiligingsaanval op de aanmelding uit te voeren. Daarnaast kunt u, als het rootaccount onvoldoende niet-afwijzing blijkt te verschaffen door meer dan één persoon in uw organisatie, ervoor kiezen de beheerder voor de beheerinterface te wijzigen.

Voorwaarden

Procedure

- 1 Voer de volgende opdracht uit om een nieuwe gebruiker te maken en deze toe te voegen aan de Virtual Appliance Management Interface-groep.

```
useradd -G vami,root gebruiker
```

- 2 Maak een wachtwoord voor de gebruiker.

```
passwd gebruiker
```

- 3 (Optioneel) Voer de volgende opdracht uit om roottoegang in de Virtual Appliance Management Interface uit te schakelen.

```
usermod -R vami root
```

Opmerking Als roottoegang tot de Virtual Appliance Management Interface wordt uitgeschakeld, is het ook niet meer mogelijk het beheerderswachtwoord, of het rootwachtwoord, uit te schakelen op het tabblad Beheer.

Boot Loader-verificatie instellen

Om een passend beveiligingsniveau te bieden, configureert u boot loader-verificatie op uw VMware virtual appliances.

Als de boot loader van het systeem geen verificatie behoeft, kunnen gebruikers met toegang tot het systeemconsole de systeemstartconfiguratie veranderen of het systeem opstarten in de modus voor één gebruiker of onderhoud, wat kan leiden tot denial of service of onbevoegde toegang tot het systeem. Omdat boot loader-verificatie niet standaard ingesteld is op de VMware virtual appliances, moet u een GRUB-wachtwoord creëren om dit te configureren.

Procedure

- 1 Controleer of er een opstartwachtwoord bestaat door de regel `password --md5 <password-hash>` in het bestand `/boot/grub/menu.lst` op uw virtual appliances te zoeken.
- 2 Als er geen wachtwoord bestaat, voer dan de opdracht `# /usr/sbin/grub-md5-crypt` uit op uw virtual appliance.

Er wordt een MD5-wachtwoord gegenereerd, en de opdracht levert de md5 Hash-uitvoer.

- 3 Voeg het wachtwoord toe aan het bestand `menu.lst` door de opdracht `# password --md5 <hash from grub-md5-crypt>` uit te voeren.

NTP configureren

Voor tijdsourcing schakelt u tijdsynchronisatie van de host uit en gebruikt u het Network Time Protocol (NTP) voor de vRealize Automation-toepassing.

De NTP-daemon op de vRealize Automation-toepassing levert gesynchroniseerde tijdservices. NTP is standaard uitgeschakeld dus u moet deze handmatig configureren. Gebruik indien mogelijk NTP in productieomgevingen voor het volgen van gebruikersacties en het detecteren van potentiële aanvallen en inbraken door middel van accurate audits en logboekregistratie. Raadpleeg de website van NTP voor informatie over NTP-beveiligingsberichten.

De NTP-configuratie bevindt zich in de map `/etc/` in elke toepassing. U kunt de NTP-service voor de vRealize Automation-toepassing inschakelen en tijdsservers toevoegen op het tabblad **Beheer** in de beheerinterface van de virtual appliance.

Procedure

- 1 Open het configuratiebestand `/etc/ntp.conf` op de hostmachine van uw virtual appliance in een teksteditor.
- 2 Stel het eigendom van het bestand in op **root:root**.
- 3 Stel de rechten in op **0640**.
- 4 Het risico van een Denial of Service Amplification-aanval op de NTP-service kan worden verholpen door het bestand `/etc/ntp.conf` te openen en te controleren of de beperkingsregels in het bestand voorkomen.

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

- 5 Sla gemaakte wijzigingen op en sluit het bestand.

TLS voor gegevens in overdracht configureren voor de vRealize Automation-toepassing

Zorg ervoor dat uw vRealize Automation-implementatie gebruikmaakt van sterke TLS-protocollen voor veilige transmissiekanalen voor onderdelen van de vRealize Automation-toepassing.

Omwille van prestaties is TLS niet ingeschakeld voor localhost-verbindingen tussen bepaalde toepassingservices. Schakel TLS in voor alle localhost-communicatie waar uitgebreide bescherming is vereist.

Belangrijk Als u TLS op de load balancer beëindigt, dient u onveilige protocollen, zoals SSLv2, SSLv3 en TLS 1.0 op alle load balancers uit te schakelen.

TLS inschakelen op localhost-configuratie

Standaard maakt bepaalde localhost-communicatie geen gebruik van TLS. U kunt TLS inschakelen voor alle localhost-verbindingen voor nog meer veiligheid.

Procedure

- 1 Maak verbinding met de vRealize Automation-toepassing met behulp van SSH.

2 Stel de rechten voor de vcac-keystore in met de volgende opdrachten:

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

3 Update de HAProxy-configuratie.

- a Open het HAProxy-configuratiebestand op `/etc/haproxy/conf.d` en kies de service `20-vcac.cfg`.

- b Zoek de regels die de volgende tekenreeks bevatten:

```
server local 127.0.0.1... en voeg het volgende toe aan het einde van deze regels: ssl verify
none
```

Dit gedeelte bevat tevens de volgende vergelijkbare regels:

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

- c Wijzig de poort voor backend-horizon van 8080 naar 8443.

4 Haal het wachtwoord van keystorePass op.

- a Zoek de eigenschap `certificate.store.password` in het bestand `/etc/vcac/security.properties`.

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

- b Gebruik de volgende opdracht om de waarde te ontsleutelen:

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

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

5 Configureer de vRealize Automation-service

- a Open het bestand `/etc/vcac/server.xml`.
- b Voeg het volgende kenmerk toe aan de Connector-tag, waarbij u `certificate.store.password` vervangt door de `certificate.store.password`-waarde die staat 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 Configureer de vRealize Orchestrator-service

- a Open het bestand `/etc/vco/app-server.xml`
- b Voeg het volgende kenmerk toe aan de Connector-tag, waarbij u `certificate.store.password` vervangt door de `certificate.store.password`-waarde die staat 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 Start de vRealize Orchestrator, vRealize Automation en haproxy-services opnieuw.

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

Opmerking Als de vco-server niet opnieuw wordt gestart, start u de hostcomputer opnieuw op.

8 Configureer de beheerinterface van de virtual appliance.

U kunt de status van services weergeven door de volgende opdracht uit te voeren op de virtual appliance van vRealize Automation.

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

Opmerking Als u SSL inschakelt in de beheerinterface van de virtual appliance, kan de status van de vRealize Automation-services niet worden weergegeven op het tabblad Services.

- a Open het bestand `/opt/vmware/share/htdocs/service/café-services/services.py`.
- b Wijzig de regel `conn = httpLib.HTTP()` naar `conn = httpLib.HTTPS()` om de veiligheid te vergroten.

Federal Information Processing Standard (FIPS) 140-2-compliance inschakelen

De vRealize Automation-toepassing gebruikt nu voor alle inkomende en uitgaande netwerkverkeer de gecertificeerde Federal Information Processing Standard (FIPS) 140-2-versie van OpenSSL voor gegevensoverdracht via TLS.

U kunt de FIPS-modus in- of uitschakelen in de beheerinterface van de vRealize Automation-toepassing. U kunt FIPS ook met behulp van de volgende opdrachten configureren vanaf de opdrachtregel (indien u bent aangemeld als root):

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

Indien FIPS is ingeschakeld, gebruikt inkomend en uitgaand netwerkverkeer van de vRealize Automation-toepassing op poort 443 versleuteling die voldoet aan FIPS 140–2. Ongeacht de FIPS-instelling maakt vRealize Automation gebruik van AES–256 om beveiligde gegevens van de vRealize Automation-toepassing te beschermen.

Opmerking Op dit moment schakelt vRealize Automation slechts gedeeltelijk FIPS-compliance in, omdat bepaalde interne onderdelen nog niet gebruikmaken van gecertificeerde cryptografische modules. In gevallen waar gecertificeerde modules nog niet zijn geïmplementeerd, wordt de op AES-256 gebaseerde encryptie gebruikt in alle cryptografische algoritmes.

Opmerking Met de volgende procedure wordt de fysieke machine opnieuw opgestart als u de configuratie wijzigt.

Procedure

- 1 Meld u aan als rootgebruiker bij de beheerinterface van de vRealize Automation-toepassing.
`https://vrealize-automation-appliance-FQDN:5480`
- 2 Selecteer **vRA > Hostinstellingen**.
- 3 Klik op de knop onder de kop Actie rechtsboven om FIPS in- of uit te schakelen.
- 4 Klik op **Ja** om de vRealize Automation-toepassing opnieuw te starten.

Controleren of SSLv3, TLS 1.0 en TLS 1.1 zijn uitgeschakeld

Controleer als onderdeel van het verhardingsproces of de geïnstalleerde vRealize Automation-toepassing gebruik maakt van beveiligde transmissiekanalen.

Opmerking U kunt de bewerking Deelnemen aan cluster niet uitvoeren na het uitschakelen van TLS 1.0/1.1 en het inschakelen van TLS 1.2.

Voorwaarden

Voltooi [TLS inschakelen op localhost-configuratie](#).

Procedure

- 1 Controleer of SSLv3, TLS 1.0 en TLS 1.1 zijn uitgeschakeld in de https-handlers voor HAProxy op vRealize Automation-toepassing.

Lees dit bestand	Controleer of het volgende aanwezig is	Op de juiste regel als weergegeven
/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 Start de service opnieuw op.

```
service haproxy restart
```

- 3 Open het bestand /opt/vmware/etc/lighttpd/lighttpd.conf en controleer of de juiste uitschakelmogelijkheden worden weergegeven.

Opmerking Er is geen instructie voor het uitschakelen van TLS 1.0 of TLS 1.1 in Lighttpd. De beperking op het gebruik van TLS 1.0 en TLS 1.1 kan gedeeltelijk worden verholpen door ervoor te zorgen dat OpenSSL geen codesuites van TLS 1.0 en TLS 1.1 gebruikt.

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

- 4 Controleer of SSLv3, TLS 1.0 en TLS 1.1 uitgeschakeld zijn voor de Console Proxy op de vRealize Automation-toepassing.
 - a Bewerk het bestand /etc/vcac/security.properties door de volgende regel toe te voegen of te bewerken:


```
consoleproxy.ssl.server.protocols = TLSv1.2
```
 - b Start de server opnieuw op door de volgende opdracht uit te voeren:


```
service vcac-server restart
```
- 5 Controleer of SSLv3, TLS 1.1 en TLS 1.0 zijn uitgeschakeld voor de vCO-service.
 - a Zoek de tag <Connector> in het bestand /etc/vco/app-server/server.xml en voeg het volgende kenmerk toe:


```
sslEnabledProtocols = "TLSv1.2"
```
 - b Start de vCO-service nogmaals door de volgende opdracht uit te voeren.


```
service vco-server restart
```

6 Controleer of SSLv3, TLS 1.1 en TLS 1.0 zijn uitgeschakeld voor de vRealize Automation-service.

- a Voeg de volgende kenmerken toe aan de tag <Connector> in het bestand /etc/vcac/server.xml

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

- b Start de vRealize Automation-service nogmaals door de volgende opdracht uit te voeren:

```
service vcac-server restart
```

7 Controleer of SSLv3, TLS 1.1 en TLS 1.0 zijn uitgeschakeld voor RabbitMQ.

Open het bestand /etc/rabbitmq/rabbitmq.config en controleer of {versions, ['tlsv1.2']} aanwezig is in de secties ssl and ssl_options.

```
[
  {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 Start de RabbitMQ-server opnieuw.

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

9 Controleer of SSLv3, TLS 1.1 en TLS 1.0 zijn uitgeschakeld voor de vIDM-service.

Open het bestand opt/vmware/horizon/workspace/conf/server.xml voor iedere instantie van de connector met SSLEnabled="true" en zorg dat de volgende regel in het bestand staat.

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

TLS-coderingssuites voor vRealize Automation-onderdelen configureren

Voor maximale veiligheid moet u vRealize Automation-onderdelen configureren zodat hierin sterke codes worden gebruikt.

De versleutelingscode die tussen de server en de browser wordt onderhandeld, bepaalt hoe sterk de versleuteling is die wordt gebruikt in een TLS-sessie.

Schakel zwakke codes in vRealize Automation-onderdelen uit om ervoor te zorgen dat alleen sterke codes worden geselecteerd. Configureer de server zodat deze alleen sterke codes ondersteunt en dat er voldoende grote codes worden gebruikt. Configureer alle codes ook in een passende volgorde.

Schakel coderingssuites uit die geen verificatie bieden, zoals de coderingssuites NULL, aNULL of eNULL. Schakel ook anonieme Diffie-Hellman-sleuteluitwisseling (ADH) uit, codes op exportniveau (EXP, codes met DES), sleutels van minder dan 128 bit voor het versleutelen van nettoladingverkeer, het gebruik van MD5 als hashing-mechanisme voor nettoladingverkeer, IDEA-coderingssuites en RC4-coderingssuites. Zorg ook dat coderingssuites die gebruikmaken van Diffie-Hellman-sleuteluitwisseling (DHE) zijn uitgeschakeld.

Zie het [Knowledge Base-artikel 2146570](#) voor meer informatie over het uitschakelen van TLS.

Zwakke codes in HA-proxy

Beoordeel de codes van de proxy-service voor hoge beschikbaarheid van de vRealize Automation-toepassing op basis van de lijst met acceptabele codes en schakel alle codes uit die als zwak worden beschouwd.

Schakel coderingssuites uit die geen verificatie bieden, zoals de coderingssuites NULL, aNULL of eNULL. Schakel ook anonieme Diffie-Hellman-sleuteluitwisseling (ADH) uit, codes op exportniveau (EXP, codes met DES), sleutels van minder dan 128 bit voor het versleutelen van nettoladingverkeer, het gebruik van MD5 als hashing-mechanisme voor nettoladingverkeer, IDEA-coderingssuites en RC4-coderingssuites.

Procedure

- 1 Bekijk de codevermeldingen in het bestand `/etc/haproxy/conf.d/20-vcac.cfg` van de bindende richtlijn en schakel alle codes uit die als zwak beschouwd worden.

```
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
```

- 2 Bekijk de codevermeldingen in het bestand `/etc/haproxy/conf.d/30-vro-config.cfg` van de bindende richtlijn en schakel alle codes uit die als zwak beschouwd worden.

```
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
```

Zwakke codes uitschakelen in de proxy-service van de console voor de vRealize Automation-toepassingvRealize Automation-toepassing

Beoordeel de codes van de proxy-service van de console voor de vRealize Automation-toepassing op basis van de lijst met acceptabele codes en schakel alle codes uit die als zwak worden beschouwd.

Schakel coderingssuites uit die geen verificatie bieden, zoals de coderingssuites NULL, aNULL of eNULL. Schakel ook anonieme Diffie-Hellman-sleuteluitwisseling (ADH) uit, codes op exportniveau (EXP, codes met DES), sleutels van minder dan 128 bit voor het versleutelen van nettoladingverkeer, het gebruik van MD5 als hashing-mechanisme voor nettoladingverkeer, IDEA-coderingssuites en RC4-coderingssuites.

Procedure

- 1 Open het bestand `/etc/vcac/security.properties` in een teksteditor.
- 2 Voeg een regel toe aan het bestand om de ongewenste codesuites uit te schakelen.

Gebruik een variatie op de volgende regel:

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

Als u bijvoorbeeld de AES 128- en AES 256-codeersuites wilt uitschakelen, voegt u de volgende regel toe:

```
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
```

- 3 Start de server opnieuw op met de volgende opdracht.

```
service vcac-server restart
```

Zwakke codes in vRealize Automation-toepassing vCO-service

Beoordeel de codes van de vRealize Automation-toepassing vCO-service op basis van de lijst met acceptabele codes en schakel alle codes uit die als zwak worden beschouwd.

Schakel coderingssuites uit die geen verificatie bieden, zoals de coderingssuites NULL, aNULL of eNULL. Schakel ook anonieme Diffie-Hellman-sleuteluitwisseling (ADH) uit, codes op exportniveau (EXP, codes met DES), sleutels van minder dan 128 bit voor het versleutelen van nettoladingverkeer, het gebruik van MD5 als hashing-mechanisme voor nettoladingverkeer, IDEA-coderingssuites en RC4-coderingssuites.

Procedure

- 1 Zoek de tag `<Connector>` in het bestand `/etc/vco/app-server/server.xml`.
- 2 Bewerk het codekenmerk of voeg het toe om de ontsleutelde codesuites te gebruiken.

Zie het volgende voorbeeld:

```
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"
```

Zwakke codes in de vRealize Automation-toepassing RabbitMQ-service uitschakelen

Beoordeel de codes van de vRealize Automation-toepassing RabbitMQ-service op basis van de lijst met acceptabele codes en schakel alle codes uit die als zwak worden beschouwd.

Schakel coderingssuites uit die geen verificatie bieden, zoals de coderingssuites NULL, aNULL of eNULL. Schakel ook anonieme Diffie-Hellman-sleuteluitwisseling (ADH) uit, codes op exportniveau (EXP, codes met DES), sleutels van minder dan 128 bit voor het versleutelen van nettoladingverkeer, het gebruik van MD5 als hashing-mechanisme voor nettoladingverkeer, IDEA-coderingssuites en RC4-coderingssuites.

Procedure

1. Evaluateer de ondersteunde coderingssuites door de opdracht `# /usr/sbin/rabbitmqctl eval 'ssl:cipher_suites()'` uit te voeren.

De in het volgende voorbeeld geretourneerde codes vertegenwoordigen uitsluitend de ondersteunde codes. De RabbitMQ-server maakt geen gebruik van deze codes en kondigt ze ook niet aan, tenzij hij is geconfigureerd om dit te doen in het bestand `rabbitmq.config`.

```
[ "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. Selecteer ondersteunde codes die voldoen aan de beveiligingsvereisten van uw organisatie.

Om bijvoorbeeld alleen `ECDHE-ECDSA-AES128-GCM-SHA256` & `ECDHE-ECDSA-AES256-GCM-SHA384` toe te staan, bekijkt u het bestand `/etc/rabbitmq/rabbitmq.config` en voegt u de volgende regel toe aan `ssl` en `ssl_options`.

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

3. Start de RabbitMQ-server opnieuw op met de volgende opdracht.

```
service rabbitmq-server restart
```

De beveiliging van Data-at-Rest controleren

De beveiliging van databasegebruikers en -accounts voor vRealize Automation controleren.

Postgres-gebruiker

Het Postgres Linux-gebruikersaccount is gekoppeld aan de superuser-accountrol van de postgres-database. Standaard is dit een vergrendeld account. Dit is de veiligste configuratie voor deze gebruiker, omdat het alleen toegankelijk is vanaf de rootgebruikeraccount. Ontgrendel dit gebruikersaccount niet.

Gebruikersaccountrollen database

De standaard gebruikersaccountrollen voor postgres mogen niet gebruikt worden voor gebruik buiten de toepassingsfunctionaliteit. Om niet-standaard databasecontrole of rapportage-activiteiten te ondersteunen moet een extra account gemaakt worden dat voldoende beveiligd is met een wachtwoord.

Voer het volgende script in de opdrachtregel uit:

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

Hiermee wordt een nieuwe gebruiker met een door de gebruiker aangemaakt wachtwoord toegevoegd.

Opmerking Dit script moet uitgevoerd worden in de master postgres-database in gevallen wanneer master-slave HA postgres-installatie geconfigureerd is.

PostgreSQL-clientverificatie configureren

Controleer of de vRealize Automation-toepassing PostgreSQL-database niet is geconfigureerd voor de verificatie van de lokale vertrouwensrelatie. Met zo'n configuratie zou iedere lokale gebruiker, inclusief de superuser van de database, zonder wachtwoord toegang kunnen krijgen als willekeurige PostgreSQL-gebruiker.

Opmerking Gebruik de account Postgres-superuser voor de lokale vertrouwensrelatie.

De md5-verificatiemethode wordt aangeraden omdat deze versleutelde wachtwoorden verzendt.

De instellingen voor de clientverificatiemethode staan in het bestand `/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

```

Als u het bestand `pg_hba.conf` bewerkt, moet u de Postgres-server opnieuw starten door de volgende opdrachten uit te voeren. Daarna zijn de veranderingen van kracht.

```

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

```

vRealize Automation-toepassingsbronnen configureren

Bekijk vRealize Automation-toepassingsbronnen en beperk de bestandsrechten.

Procedure

- 1 Voer de volgende opdracht uit om te controleren of bestanden met SUID- en GUID-bits correct zijn gedefinieerd.

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

De volgende lijst wordt weergegeven.

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 Voer de volgende opdracht uit om te controleren of alle bestanden in de virtual appliance een eigenaar hebben.

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

- 3 Gebruik de volgende opdracht te bepalen of geen van de bestandsrechten voor de virtual appliance alle gebruikers wijzigingsmogelijkheden geven.

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

- 4 Voer de volgende opdracht uit om te controleren of alleen de vcac-gebruiker de juiste bestanden bezit.

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

Als er geen resultaten worden weergegeven, dan zijn alle juiste bestanden alleen in het bezit van de vcac-gebruiker.

- 5 Controleer of de volgende bestanden alleen te wijzigen zijn door de vcac-gebruiker.

```
/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
```

Controleer ook de volgende bestanden en submappen

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

- 6 Controleer of alleen de vcac- of hoofdgebruiker de juiste bestanden kan lezen in de volgende mappen en submappen.

```
/etc/vcac/
/var/log/vcac/*
```

```
/var/lib/vcac/*
```

```
/var/cache/vcac/*
```

- 7 Controleer of de juiste bestanden alleen in het bezit zijn van de vco- of hoofdgebruiker, zoals weergegeven in de volgende mappen en submappen.

```
/etc/vco/
```

```
/var/log/vco/*
```

```
/var/lib/vco/*
```

```
/var/cache/vco/*
```

- 8 Controleer of de juiste bestanden alleen schrijfbaar zijn door de vco- of hoofdgebruiker, zoals weergegeven in de volgende mappen en submappen.

```
/etc/vco/
```

```
/var/log/vco/*
```

```
/var/lib/vco/*
```

```
/var/cache/vco/*
```

- 9 Controleer of de juiste bestanden alleen te lezen zijn door de vco- of hoofdgebruiker, zoals weergegeven in de volgende mappen en submappen.

```
/etc/vco/
```

```
/var/log/vco/*
```

```
/var/lib/vco/*
```

```
/var/cache/vco/*
```

Configuratie van consoleproxy aanpassen

U kunt de externe consoleconfiguratie van vRealize Automation omwille van de probleemoplossing of organisatorische redenen aanpassen.

Als u vRealize Automation installeert, configureert of onderhoudt, kunt u sommige instellingen wijzigen om problemen op te lossen en fouten op te sporen. Registreer en controleer alle gemaakte wijzigingen om ervoor te zorgen dat de toepasselijke onderdelen goed beveiligd zijn voor het vereiste gebruik. Ga niet over tot productie als u niet zeker weet dat uw configuratiewijzigingen voldoende beveiligd zijn.

VMware Remote Console-ticketvervaldata aanpassen

U kunt de geldigheidsperiode voor externe consoletickets die worden gebruikt bij het opzetten van VMware Remote Console-verbindingen aanpassen.

Als een gebruiker een VMware Remote Console-verbinding maakt, wordt een eenmalige referentie opgehaald voor een specifieke verbinding met een virtual machine. U kunt de ticketvervaldatum instellen op een bepaalde tijdsduur in minuten.

Procedure

- 1 Open het bestand `/etc/vcac/security.properties` in een teksteditor.
- 2 Voeg een regel met de indeling `consoleproxy.ticket.validitySec=30` toe aan het bestand.
In deze regel specificeert de numerieke waarde het aantal minuten voordat het ticket vervalst.
- 3 Sla het CSV-bestand op en sluit het.
- 4 Start de vcac-server opnieuw met gebruikmaking van de opdracht `/etc/init.d/vcac-server restart`.

De ticketvervaldatum wordt teruggezet op de opgegeven tijdsduur in minuten.

Serverpoort van de consoleproxy aanpassen

U kunt de poort waarop de VMware Remote Console-consoleproxy berichten zoekt aanpassen.

Procedure

- 1 Open het bestand `/etc/vcac/security.properties` in een teksteditor.
- 2 Voeg een regel met de indeling `consoleproxy.service.port=8445` toe aan het bestand.
De numerieke waarde specificeert het poortnummer van de consoleproxyserver, in dit geval 8445.
- 3 Sla het CSV-bestand op en sluit het.
- 4 Start de vcac-server opnieuw met gebruikmaking van de opdracht `/etc/init.d/vcac-server restart`.

De proxyservicepoort wordt ingesteld op het gespecificeerde poortnummer.

X-XSS-Protection-reactieheader configureren

Voeg de reactieheader X-XSS-Protection toe aan het HAProxy-configuratiebestand.

Procedure

- 1 Open `/etc/haproxy/conf.d/20-vcac.cfg` om te bewerken.
- 2 Voeg de volgende regels toe in de front-endsectie.

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

- 3 Laad de HAProxy-configuratie opnieuw met de volgende opdracht.

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

Reactieheader X-Content-Type-Options configureren

Voeg de reactieheader X-Content-Type-Options toe aan de HAProxy-configuratie.

Procedure

- 1 Open `/etc/haproxy/conf.d/20-vcac.cfg` om te bewerken.
- 2 Voeg de volgende regels toe in de front-endsectie.

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

- 3 Laad de HAProxy-configuratie opnieuw met de volgende opdracht.

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

De reactieheader van de HTTP Strict Transport-beveiliging configureren

Voeg de reactieheader van de HSTS (HTTP Strict Transport) toe aan de HAProxy-configuratie.

Procedure

- 1 Open `/etc/haproxy/conf.d/20-vcac.cfg` om te bewerken.
- 2 Voeg de volgende regels toe in de front-endsectie.

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

- 3 Laad de HAProxy-configuratie opnieuw met de volgende opdracht.

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

X-Frame-Options-reactieheader configureren

De X-Frame-Options-reactieheader wordt in bepaalde gevallen twee keer weergegeven.

De X-Frame-Options-reactieheader kan twee keer worden weergegeven omdat de vIDM-service deze header zowel aan de back-end als aan HAProxy toevoegt. Met een juiste configuratie voorkomt u dat deze twee keer wordt weergegeven.

Procedure

- 1 Open `/etc/haproxy/conf.d/20-vcac.cfg` om te bewerken.
- 2 Zoek de volgende regel in de front-endsectie.

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

- 3 Voeg de volgende regels toe vóór de regel die u in de vorige stap hebt gevonden:

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

- 4 Laad de HAProxy-configuratie opnieuw met de volgende opdracht.

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

Serverresponsheaders configureren

Als best practice voor beveiliging moet u uw vRealize Automation-systeem configureren om informatie die beschikbaar is voor mogelijke aanvallers te beperken.

Beperk de gedeelde informatie over de identiteit en versie van uw systeem zoveel mogelijk. Hackers en mensen die kwaad willen kunnen deze informatie gebruiken om doelgerichte aanvallen op te zetten tegen uw webserver of versie.

De reactieheader van de Lighttpd-server configureren

De aanbevolen procedure is een blanco serverheader te maken voor de lighttpd-header van de vRealize Automation-toepassing.

Procedure

- 1 Open het bestand `/opt/vmware/etc/lighttpd/lighttpd.conf` in een teksteditor.
- 2 Voeg `server.tag = " "` toe aan het bestand.
- 3 Sla uw wijzigingen op en sluit het bestand.
- 4 Start de lighttpd-server opnieuw op door de opdracht `# /opt/vmware/etc/init.d/vami-lighttpd restart` uit te voeren.

De TCServer-reactieheader voor de vRealize Automation-toepassing configureren

De aanbevolen procedure is een aangepaste blanco serverheader te maken voor de TCServer-reactieheader die wordt gebruikt met de vRealize Automation-toepassing om de mogelijkheid te beperken dat kwaadwillenden waardevolle gegevens stelen.

Procedure

- 1 Open het bestand `/etc/vco/app-server/server.xml` in een teksteditor.
- 2 Voeg in elk `<Connector>`-element `server=" "` toe.
Bijvoorbeeld: `<Connector protocol="HTTP/1.1" server="" />`.
- 3 Sla uw wijzigingen op en sluit het bestand.
- 4 Start de server opnieuw op met de volgende opdracht.
`service vco-server restart`

De reactieheader van de Internet Information Services-server configureren

De aanbevolen procedure is een aangepaste blanco serverheader te maken voor de Internet Information Services-server (IIS) die wordt gebruikt met de Identity Appliance om de mogelijkheid dat kwaadwillenden waardevolle gegevens stelen, te beperken.

Procedure

- 1 Open het bestand C:\Windows\System32\inetsrv\urlscan\UrlScan.ini in een teksteditor.
- 2 Zoek RemoveServerHeader=0 en wijzig deze in RemoveServerHeader=1.
- 3 Sla uw wijzigingen op en sluit het bestand.
- 4 Start de server opnieuw op door de opdracht `iisreset` uit te voeren.

Wat nu te doen

Schakel de IIS X-Powered By-header uit door HTTP-reactieheaders te verwijderen uit de lijst in de IIS-beheerconsole.

- 1 Open de IIS-beheerconsole.
- 2 Open de HTTP-reactieheader en verwijder deze van de lijst.
- 3 Start de server opnieuw op door de opdracht `iisreset` uit te voeren.

Sessie-time-out vRealize Automation-toepassing instellen

Configureer de sessie-time-out-instellingen op de vRealize Automation-toepassing in overeenstemming met het beveiligingsbeleid van uw bedrijf.

De vRealize Automation-toepassing standaard sessie-time-out bij inactiviteit van gebruikers is 30 minuten. Om deze time-outwaarde aan te passen aan het beveiligingsbeleid van uw bedrijf, bewerkt u het bestand `web.xml` op uw vRealize Automation-toepassing-hostmachine.

Procedure

- 1 Open het bestand `/usr/lib/vcac/server/webapps/vcac/WEB-INF/web.xml` in een teksteditor.
- 2 Zoek `session-config` en stel de waarde voor sessie-time-out in. Zie het volgende codevoorbeeld.

```
<!-- 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 Start de server opnieuw door de volgende opdracht uit te voeren.

```
service vcac-server restart
```

Niet-essentiële software beheren

Om veiligheidsrisico's te minimaliseren, verwijdert u niet-essentiële software van uw vRealize Automation-hostmachines of configureert u ze.

Configureer alle software die u niet verwijdt zoals omschreven is in de aanbevelingen van de fabrikant en geadviseerde beveiligingsmaatregelen om de kans dat deze software beveiligingsproblemen veroorzaakt te minimaliseren.

De handler voor USB-massaopslag beveiligen

Beveilig de handler voor USB-massaopslag om te voorkomen dat deze wordt gebruikt als USB-apparaathandler op hostmachines van de VMware virtual appliances. Kwaadwillenden kunnen deze handler gebruiken om uw systeem aan te vallen.

Procedure

- 1 Open het bestand `/etc/modprobe.conf.local` in een teksteditor.
- 2 Controleer of de regel `install usb-storage /bin/true` in het bestand staat.
- 3 Sla het CSV-bestand op en sluit het.

De Bluetooth-protocolhandler beveiligen

Beveilig de Bluetooth-protocolhandler op de hostmachines van uw virtual appliances om te voorkomen dat mogelijke aanvallers deze uitbuiten.

Het is niet nodig het Bluetooth-protocol te koppelen aan de netwerkstack. Hierdoor wordt de host extra blootgesteld aan mogelijke aanvallen.

Procedure

- 1 Open het bestand `/etc/modprobe.conf.local` in een teksteditor.
- 2 Controleer of de volgende regel in dit bestand staat.

```
install bluetooth /bin/true
```
- 3 Sla het CSV-bestand op en sluit het.

Het Stream Control Transmission-protocol beveiligen

Voorkom dat het protocol Stream Control Transmission (SCTP) standaard op uw systeem geladen wordt. Kwaadwillenden kunnen dit protocol gebruiken om uw systeem aan te vallen.

Configureer uw systeem zo dat voorkomen wordt dat de Stream Control Transmission Protocol (SCTP)-module geladen wordt, tenzij dit absoluut noodzakelijk is. SCTP is een ongebruikt IETF-standaard transportlaagprotocol. Door dit protocol aan de netwerkstack te koppelen, wordt de host extra blootgesteld aan mogelijke aanvallen. Lokale processen zonder rechten kunnen ervoor zorgen dat de kernel dynamisch een protocolhandler laadt door het protocol te gebruiken om een socket te openen.

Procedure

- 1 Open het bestand `/etc/modprobe.conf.local` in een teksteditor.
- 2 Controleer of de volgende regel in dit bestand staat.

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


- 3 Sla het CSV-bestand op en sluit het.

Het Datagram Congestion-protocol beveiligen

Voorkom als onderdeel van het verharden van uw systeem dat het Datagram Congestion Protocol (DCCP) standaard op de hostmachines van uw virtual appliances geladen wordt. Kwaadwillenden kunnen dit protocol gebruiken om uw systeem aan te vallen.

Voorkom dat de Datagram Congestion Control Protocol (DCCP)-module geladen wordt, tenzij dit absoluut noodzakelijk is. DCCP is een voorgesteld transportlaagprotocol dat niet wordt gebruikt. Door dit protocol aan de netwerkstack te koppelen, wordt de host extra blootgesteld aan mogelijke aanvallen. Lokale processen zonder rechten kunnen ervoor zorgen dat de kernel dynamisch een protocolhandler laadt door het protocol te gebruiken om een socket te openen.

Procedure

- 1 Open het bestand `/etc/modprobe.conf.local` in een teksteditor.
- 2 Controleer of de DCCP-regels in het bestand staan.

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

- 3 Sla het CSV-bestand op en sluit het.

Network Bridging beveiligen

Voorkom dat de network bridging-module standaard op uw systeem geladen wordt. Kwaadwillenden kunnen deze module gebruiken om uw systeem aan te vallen.

Configureer uw systeem om te voorkomen dat het netwerk deze module laadt, tenzij het absoluut noodzakelijk is. Mogelijke aanvallers kunnen de module gebruiken om netwerkpartities en -beveiliging te omzeilen.

Procedure

- 1 Voer de volgende opdracht uit op iedere VMware virtual appliance-hostmachine.

```
# rmmod bridge
```

- 2 Open het bestand `/etc/modprobe.conf.local` in een teksteditor.
- 3 Controleer of de volgende regel in dit bestand staat.

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

- 4 Sla het CSV-bestand op en sluit het.

Het Reliable Datagram Sockets-protocol beveiligen

Voorkom als onderdeel van het verharden van uw systeem dat het Reliable Datagram Sockets Protocol (RDS) standaard op de hostmachines van uw virtual appliances geladen wordt. Kwaadwillenden kunnen dit protocol gebruiken om uw systeem aan te vallen.

Door het Reliable Datagram Sockets (RDS)-protocol aan de netwerkstack te koppelen, wordt de host extra blootgesteld aan mogelijke aanvallen. Lokale processen zonder rechten kunnen ervoor zorgen dat het systeem dynamisch een protocolhandler laadt door het protocol te gebruiken om een socket te openen.

Procedure

- 1 Open het bestand `/etc/modprobe.conf.local` in een teksteditor.
- 2 Controleer of de regel `install rds /bin/true` in dit bestand staat.
- 3 Sla het CSV-bestand op en sluit het.

Het Secure Transparent Inter-Process Communication-protocol beveiligen

Voorkom als onderdeel van het verharderen van uw systeem dat het Transparent Inter-Process Communication-protocol (TIPC) standaard op de hostmachines van uw virtual appliances geladen wordt. Kwaadwillenden kunnen dit protocol gebruiken om uw systeem aan te vallen.

Door het Transparent Inter-Process Communications (TIPC)-protocol aan de netwerkstack te koppelen, wordt de host extra blootgesteld aan mogelijke aanvallen. Lokale processen zonder rechten kunnen ervoor zorgen dat de kernel dynamisch een protocolhandler laadt door het protocol te gebruiken om een socket te openen.

Procedure

- 1 Open het bestand `/etc/modprobe.conf.local` in een teksteditor.
- 2 Controleer of de regel `install tipc /bin/true` in dit bestand staat.
- 3 Sla het CSV-bestand op en sluit het.

Het Internetwork Packet Exchange-protocol beveiligen

Voorkom dat het protocol Internetwork Packet Exchange (IPX) standaard op uw systeem geladen wordt. Kwaadwillenden kunnen dit protocol gebruiken om uw systeem aan te vallen.

Voorkom dat de module Internetwork Packet Exchange (IPX) Protocol geladen wordt, tenzij dit absoluut noodzakelijk is. IPX-protocol is een verouderd netwerklaagprotocol. Door dit protocol aan de netwerkstack te koppelen, wordt de host extra blootgesteld aan mogelijke aanvallen. Lokale processen zonder rechten kunnen ervoor zorgen dat het systeem dynamisch een protocolhandler laadt door het protocol te gebruiken om een socket te openen.

Procedure

- 1 Open het bestand `/etc/modprobe.conf.local` in een teksteditor.
- 2 Controleer of de volgende regel in dit bestand staat.

`install ipx /bin/true`
- 3 Sla het CSV-bestand op en sluit het.

Het Appletalk-protocol beveiligen

Voorkom dat het Appletalk-protocol standaard op uw systeem geladen wordt. Kwaadwillenden kunnen dit protocol gebruiken om uw systeem aan te vallen.

Voorkom dat de module Appletalk Protocol geladen wordt, tenzij dit absoluut noodzakelijk is. Door dit protocol aan de netwerkstack te koppelen, wordt de host extra blootgesteld aan mogelijke aanvallen. Lokale processen zonder rechten kunnen ervoor zorgen dat het systeem dynamisch een protocolhandler laadt door het protocol te gebruiken om een socket te openen.

Procedure

- 1 Open het bestand `/etc/modprobe.conf.local` in een teksteditor.
- 2 Controleer of de volgende regel in dit bestand staat.

```
install appletalk /bin/true
```

- 3 Sla het CSV-bestand op en sluit het.

Het DECnet-protocol beveiligen

Voorkom dat het DECnet-protocol standaard op uw systeem geladen wordt. Kwaadwillenden kunnen dit protocol gebruiken om uw systeem aan te vallen.

Voorkom dat de module DECnet Protocol geladen wordt, tenzij dit absoluut noodzakelijk is. Door dit protocol aan de netwerkstack te koppelen, wordt de host extra blootgesteld aan mogelijke aanvallen. Lokale processen zonder rechten kunnen ervoor zorgen dat het systeem dynamisch een protocolhandler laadt door het protocol te gebruiken om een socket te openen.

Procedure

- 1 Open het bestand DECnet Protocol `/etc/modprobe.conf.local` in een teksteditor.
- 2 Controleer of de volgende regel in dit bestand staat.

```
install decnet /bin/true
```

- 3 Sla het CSV-bestand op en sluit het.

De Firewire-module beveiligen

Voorkom dat de Firewire-module standaard op uw systeem geladen wordt. Kwaadwillenden kunnen dit protocol gebruiken om uw systeem aan te vallen.

Voorkom dat de Firewire-module geladen wordt, tenzij dit absoluut noodzakelijk is.

Procedure

- 1 Open het bestand `/etc/modprobe.conf.local` in een teksteditor.
- 2 Controleer of de volgende regel in dit bestand staat.

```
install ieee1394 /bin/true
```

- 3 Sla het CSV-bestand op en sluit het.

Het onderdeel Infrastructure as a Service beveiligen

Beveilig voor het verharderen van uw systeem het onderdeel vRealize Automation Infrastructure as a Service (IaaS) en de hostmachine om te voorkomen dat aanvallers hier gebruik van kunnen maken.

U moet de beveiligingsinstelling voor het onderdeel vRealize Automation Infrastructure as a Service (IaaS) en de host waarop hij staat, configureren. U moet de configuratie van andere gerelateerde onderdelen en toepassingen instellen of controleren. In sommige gevallen kunt u bestaande instellingen controleren, in andere gevallen moet u instellingen aanpassen of toevoegen om tot een juiste configuratie te komen.

NTP configureren

De aanbevolen beveiligingsprocedure is geautoriseerde tijdservers te gebruiken in plaats van het hosten van tijdssynchronisatie in een vRealize Automation-productieomgeving.

In een productieomgeving schakelt u de hosttijdsynchronisatie uit en gebruikt u geautoriseerde tijdservers om gebruikersacties nauwkeurig bij te kunnen houden en mogelijke schadelijke aanvallen en inbraak te identificeren door controles en logboekregistraties.

TLS voor Infrastructure as a Service Data-in-Transit configureren

Zorg ervoor dat uw vRealize Automation-implementatie gebruikmaakt van sterke TLS-protocollen voor veilige transmissiekanalen voor Infrastructure as a Service-onderdelen.

Secure Sockets Layer (SSL) en het recent ontwikkelde Transport Layer Security (TLS) zijn cryptografieprotocollen die mede zorgen voor systeembeveiliging tijdens netwerkcommunicatie tussen verschillende systeemonderdelen. SSL is een oudere standaard, dus veel onderdelen bieden geen adequate beveiliging meer tegen potentiële aanvallen. Eerdere SSL-protocollen, inclusief SSLv2 en SSLv3, hebben ernstige zwakke punten. Deze protocollen worden niet meer als veilig beschouwd.

Afhankelijk van het beveiligingsbeleid van uw organisatie kunt u overwegen ook TLS 1.0 uit te schakelen.

Opmerking Wanneer u TLS op de load balancer beëindigt, schakel dan ook zwakke protocollen zoals SSLv2, SSLv3 en TLS 1.0 en 1.1 uit indien nodig.

De protocollen TLS 1.1 en 1.2 voor IaaS inschakelen

Schakel het gebruik van de protocollen TLS 1.1 en 1.2 in op alle virtual machines waarop IaaS-onderdelen worden gehost en dwing dit af.

Procedure

- 1 Klik op **Start** en vervolgens op **Uitvoeren**.
- 2 Typ regedit en klik vervolgens op **OK**.
- 3 Zoek de volgende subsleutel in het register en open deze.

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

4 Controleer de volgende zaken en maak indien nodig nieuwe vermeldingen.

- Als er geen subsleutel is met de naam TLS 1.1 onder Protocollen, maakt u er een.
- Als er geen subsleutel is met de naam Client onder TLS 1.1, maakt u er een.
- Als er geen sleutel is met de naam DisabledByDefault in de subsleutel Client, maakt u er een met het type DWORD.
- Klik met de rechtermuisknop op DisabledByDefault, selecteer Aanpassen en stel de waarde ervan in op 0.
- Als er geen sleutel is met de naam Enabled in de subsleutel Client, maakt u er een met het type DWORD.
- Klik met de rechtermuisknop op Enabled, selecteer Aanpassen en stel de waarde ervan in op 1.
- Als er in TLS 1.1 geen subsleutel met de naam Server is, maakt u er een.
- Als er geen sleutel is met de naam DisabledByDefault in de subsleutel Server, maakt u er een met het type DWORD.
- Klik met de rechtermuisknop op DisabledByDefault, selecteer Aanpassen en stel de waarde ervan in op 0.
- Als er geen sleutel met de naam Enabled is in de subsleutel Server, maakt u er een met het type DWORD.
- Klik met de rechtermuisknop op Enabled, selecteer Aanpassen en stel de waarde ervan in op 1.

5 Herhaal de vorige stap voor het protocol TLS 1.2.

Opmerking Om het gebruik van TLS 1.1 en 1.2 af te dwingen, zijn aanvullende instellingen vereist, zoals beschreven in de volgende stappen.

6 Zoek de volgende subsleutel in het register en open deze.

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

7 Controleer de volgende zaken en maak indien nodig nieuwe vermeldingen.

- Als er geen DWORD-vermelding is met de naam SchUseStrongCrypto, maakt u er een en stelt u de waarde ervan in op 1.
- Als er geen DWORD-vermelding met de naam SystemDefaultTlsVersions is, maakt u er een en stelt u de waarde ervan in op 1.

8 Zoek de volgende subsleutel in het register en open deze.

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

9 Controleer de volgende zaken en maak indien nodig nieuwe vermeldingen.

- Als er geen DWORD-vermelding is met de naam SchUseStrongCrypto, maakt u er een en stelt u de waarde ervan in op 1.

- Als er geen DWORD-vermelding met de naam SystemDefaultTlsVersions is, maakt u er een en stelt u de waarde ervan in op 1.

SSL 3.0 en TLS 1.0 voor IaaS uitschakelen

Schakel SSL 3.0 en het verouderde TLS 1.0-protocol voor IaaS-onderdelen uit.

Procedure

1 Klik op **Start** en vervolgens op **Uitvoeren**.

2 Typ Regedit en klik vervolgens op **OK**.

3 Zoek de volgende subsleutel in het register en open deze.

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

4 Controleer de volgende zaken en maak indien nodig nieuwe vermeldingen.

- Als er geen subsleutel is met de naam onder SSL 3.0 onder Protocollen, maakt u er een.
- Als er geen subsleutel is met de naam Client onder SSL 3.0, maakt u er een.
- Als er geen sleutel is met de naam DisabledByDefault in de subsleutel Client, maakt u er een met het type DWORD.
- Klik met de rechtermuisknop op DisabledByDefault, selecteer Aanpassen en stel de waarde ervan in op 1.
- Klik met de rechtermuisknop op Enabled, selecteer Aanpassen en stel de waarde ervan in op 0.
- Als er geen subsleutel is met de naam Server onder SSL 3.0, maakt u er een.
- Als er geen sleutel is met de naam DisabledByDefault in de subsleutel Server, maakt u er een met het type DWORD.
- Klik met de rechtermuisknop op DisabledByDefault, selecteer Aanpassen en stel de waarde ervan in op 1.
- Als er geen sleutel is met de naam Enabled in Server, maakt u er een met het type DWORD.
- Klik met de rechtermuisknop op Enabled, selecteer Aanpassen en stel de waarde ervan in op 0.

5 Herhaal de voorgaande stappen voor het TLS 1.0-protocol.

TLS 1.0 uitschakelen voor IaaS

Configureer IaaS om groeperen te gebruiken en schakel TLS 1.0 uit voor maximale veiligheid.

Zie het Microsoft Knowledge Base-artikel <https://support.microsoft.com/en-us/kb/245030> voor meer informatie.

Procedure

- 1 IaaS configureren om groeperen te gebruiken in plaats van websockets.
 - a Update het configuratiebestand voor beheerservices C:\Program Files (x86)\VMware\vCAC\Server\ManagerService.exe.config door de volgende waarden toe te voegen in het gedeelte <appSettings>


```
<add key="Extensibility.Client.RetrievalMethod" value="Polling"/>
<add key="Extensibility.Client.PollingInterval" value="2000"/>
<add key="Extensibility.Client.PollingMaxEvents" value="128"/>
```
 - b Start de beheerservice (VMware vCloud Automation Center-service) opnieuw.
- 2 Controleer of TLS 1.0 is uitgeschakeld op de IaaS-server.
 - a Voer de registereditor uit als beheerder.
 - b Navigeer naar HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\ in het registervenster.
 - c Klik met de rechtermuisknop op Protocollen en selecteer **Nieuwe > sleutel**. Voer vervolgens **TLS 1.0** in.
 - d Klik in de navigatiestructuur met de rechtermuisknop op de sleutel TLS 1.0 die u zojuist hebt aangemaakt en selecteer in het snelmenu **Nieuwe > sleutel**. Voer vervolgens **Client** in.
 - e Klik in de navigatiestructuur met de rechtermuisknop op de sleutel TLS 1.0 die u zojuist hebt aangemaakt en selecteer in het snelmenu **Nieuwe > sleutel**. Voer vervolgens **Server** in.
 - f Klik in de navigatiestructuur, onder TLS 1.0, met de rechtermuisknop op **Client** en vervolgens op **Nieuwe > DWORD (32 bits)-waarde**. Voer aansluitend **DisabledByDefault** in.
 - g Selecteer in de navigatiestructuur, onder TLS 1.0, **Client** en dubbelklik in het rechterdeelvenster op **DisabledByDefault** DWORD. Voer vervolgens **1** in.
 - h Klik in de navigatiestructuur, onder TLS 1.0, met de rechtermuisknop op **Server** en selecteer **Nieuwe > DWORD (32 bits)-waarde**. Voer vervolgens **Enabled** in.
 - i Selecteer in de navigatiestructuur, onder TLS 1.0, **Server** en dubbelklik in het rechterdeelvenster op **Ingeschakeld** DWORD. Voer vervolgens **0** in.
 - j Start de Windows-server opnieuw op.

TLS-coderingssuites configureren

Voor maximale veiligheid moet u vRealize Automation-onderdelen configureren zodat hierin sterke codes worden gebruikt. De versleutelingscode die tussen de server en de browser wordt onderhandeld, bepaalt hoe sterk de versleuteling is die wordt gebruikt in een TLS-sessie. Schakel zwakke codes in vRealize Automation-onderdelen uit om ervoor te zorgen dat alleen sterke codes worden geselecteerd. Configureer de server zodat deze alleen sterke codes ondersteunt en dat er voldoende grote codes worden gebruikt. Configureer alle codes ook in een passende volgorde.

Coderingssuites die niet acceptabel zijn

Schakel coderingssuites uit die geen verificatie bieden, zoals de coderingssuites NULL, aNULL of eNULL. Schakel ook anonieme Diffie-Hellman-sleuteluitwisseling (ADH) uit, codes op exportniveau (EXP, codes met DES), sleutels van minder dan 128 bit voor het versleutelen van nettoladingverkeer, het gebruik van MD5 als hashing-mechanisme voor nettoladingverkeer, IDEA-coderingssuites en RC4-coderingssuites. Zorg ook dat coderingssuites die gebruikmaken van Diffie-Hellman-sleuteluitwisseling (DHE) zijn uitgeschakeld.

Zie [Knowledge Base-artikel 71094](#) voor informatie over het uitschakelen van statische sleutelcodes in vRealize Automation.

Beveiliging van hostserver controleren

Controleer als best practice voor beveiliging de beveiligingsconfiguratie van uw hostmachines voor Infrastructure as a Service (IaaS).

Microsoft biedt verschillende tools aan voor het controleren van de beveiliging op hostservermachines. Neem contact op uw met Microsoft-dealer voor advies over het beste gebruik van deze tools.

Beveiligde basis van hostserver controleren

Voer de Microsoft Baseline Security Analyzer (MBSA) uit om snel vast te stellen of uw server beschikt over de nieuwste updates of hot fixes. U kunt de MBSA gebruiken voor het installeren van ontbrekende patches van Microsoft om uw server up-to-date te houden met de beveiligingsaanbevelingen van Microsoft.

Download de nieuwste versie van de MBSA tool van de website van Microsoft.

Beveiligingsconfiguratie van hostserver controleren

Gebruik de Windows Security Configuration Wizard (SCW) en de Microsoft Security Compliance Manager (SCM) toolkit om te controleren of de hostserver veilig geconfigureerd is.

Voer de SCW uit vanuit de beheerderstools op uw Windows-server. Deze tool kan de rollen van uw server en de geïnstalleerde functies identificeren, inclusief netwerken, Windows-firewalls en registerinstellingen. Vergelijk het rapport met de nieuwste verhardingsrichtlijnen van de relevante SCM voor uw Windows-server. Op basis van de resultaten kunt u de beveiligingsinstellingen voor iedere functie aanpassen, zoals netwerkdiensten, accountinstellingen en Windows-firewalls, en de instellingen toepassen op uw server.

U vindt meer informatie over de SCW tool op de Microsoft Technet-site.

Toepassingsbronnen beschermen

Als best practice voor beveiliging moet u zorgen dat alle relevante Infrastructure as a Service-bestanden de juiste rechten hebben.

Controleer Infrastructure as a Service-bestanden aan de hand van uw Infrastructure as a Service-installatie. In de meeste gevallen moeten submappen en -bestanden voor iedere map dezelfde instellingen als de map hebben.

Map of bestand	Groep of gebruikers	Volledige controle	Wijzigen	Lezen en uitvoeren	Lezen	Schrijven
VMware\vmCAC\Agents\ <agent_name>\logs	SYSTEEM	X	X	X	X	X
	Beheerder	X	X	X	X	X
	Beheerders	X	X	X	X	X
VMware\vmCAC\Agents\ <agent_name>\temp	SYSTEEM	X	X	X	X	X
	Beheerder	X	X	X	X	X
	Beheerders	X	X	X	X	X
VMware\vmCAC\Agents\	SYSTEEM	X	X	X	X	X
	Beheerders	X	X	X	X	X
	Gebruikers			X	X	
VMware\vmCAC\Distributed Execution Manager\	SYSTEEM	X	X	X	X	X
	Beheerders	X	X	X	X	X
	Gebruikers			X	X	
VMware\vmCAC\Distributed Execution Manager\DEM\Log	SYSTEEM	X	X	X	X	X
	Beheerder	X	X	X	X	X
	Beheerders	X	X	X	X	X
VMware\vmCAC\Distributed Execution Manager\DEO\Log	SYSTEEM	X	X	X	X	X
	Beheerder	X	X	X	X	X
	Beheerders	X	X	X	X	X
VMware\vmCAC\Management Agent\	SYSTEEM	X	X	X	X	X
	Beheerders	X	X	X	X	X
	Gebruikers			X	X	
VMware\vmCAC\Server\	SYSTEEM	X	X	X	X	X
	Beheerders	X	X	X	X	X
	Gebruikers			X	X	
VMware\vmCAC\Web API	SYSTEEM	X	X	X	X	X
	Beheerders	X	X	X	X	X
	Gebruikers			X	X	

De Infrastructure as a Service-hostmachine beveiligen

De aanbevolen beveiligingsprocedure is de minimale instellingen voor uw Infrastructure as a Service-hostmachine (IaaS) te controleren op naleving van de beveiligingsrichtlijnen.

Beveilig diverse accounts, toepassingen, poorten en services op de Infrastructure as a Service-hostmachine (IaaS).

Accountinstellingen voor de servergebruiker verifiëren

Controleer of er mogelijk onnodige accounts of instellingen voor lokale gebruikers of domeingebruikers zijn. Beperk gebruikersaccounts die niet zijn gekoppeld met toepassingsfuncties tot de accounts die zijn vereist voor beheer, onderhoud en probleemoplossing. Beperk externe toegang van domeingebruikersaccounts tot het minimum dat is vereist voor onderhoud van de server. Voer strikte controles uit voor deze accounts.

Onnodige toepassingen verwijderen

Verwijder alle onnodige toepassingen van de hostservers. Onnodige toepassingen verhogen het risico op blootstelling vanwege onbekende of niet-verholpen beveiligingsproblemen.

Onnodige poorten en services uitschakelen

Controleer de firewall van de hostserver voor de lijst met open poorten. Blokkeer alle poorten die niet zijn vereist voor de werking van het IaaS-onderdeel of essentiële systemen. Zie [Poorten en protocollen configureren](#). Voer audits uit voor de services die worden uitgevoerd op uw hostserver en schakel de services die niet zijn vereist uit.

Hostnetwerkbeveiliging configureren

8

Configureer instellingen voor de netwerkinterface en -communicatie op alle VMware-hostmachines voor maximale beveiliging tegen onbekende bedreigingen.

Configureer beveiligingsinstellingen voor de netwerkinterface voor de virtual appliances van VMware en de Infrastructure as a Service-onderdelen volgens de vastgestelde beveiligingsrichtlijnen als onderdeel van een uitgebreid beveiligingsplan.

Dit hoofdstuk omvat de volgende onderwerpen:

- [Netwerkinstellingen configureren voor VMware-toepassingen](#)
- [Netwerkinstellingen voor de Infrastructure as a Service-host configureren](#)
- [Poorten en protocollen configureren](#)

Netwerkinstellingen configureren voor VMware-toepassingen

Controleer en bewerk de instellingen voor netwerkcommunicatie van de VMware-hostmachine van uw virtual appliances om er zeker van te zijn dat de hostmachines alleen veilige en essentiële communicatie ondersteunen.

Controleer de netwerk-IP-protocolconfiguratie van uw VMware-hostmachines en configureer netwerkinstellingen volgens de beveiligingsrichtlijnen. Schakel alle niet-essentiële communicatieprotocollen uit.

Toegang van gebruikers tot netwerkinterfaces voorkomen

Als best practice voor beveiliging mag u gebruikers alleen de systeemrechten geven die ze nodig hebben om hun werkzaamheden uit te voeren op hostmachines van VMware-toepassingen.

Gebruikersaccounts met rechten toestaan netwerkinterfaces te manipuleren, kan leiden tot het omzeilen van netwerkbeveiligingsmechanismen of denial of service. Beperk de mogelijkheid om netwerkinterface-instellingen te wijzigen tot bevoegde gebruikers.

Procedure

- 1 Voer de volgende opdracht uit op iedere hostmachine van de VMware-toepassing.

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

- 2 Zorg dat iedere interface is ingesteld op NO

Wachtrijgrootte TCP Backlog instellen

Om verdediging te bieden tegen schadelijke aanvallen, configureert u een standaard wachtrijgrootte voor TCP backlog op de VMware-toepassingshostmachines.

Stel de wachtrijgroottes voor TCP backlog in op een passende standaardgrootte om te beschermen tegen TCP denial of service-aanvallen. De aanbevolen standaardinstelling is 1280.

Procedure

- 1 Voer de volgende opdracht uit op iedere VMware-toepassingshostmachine.

```
# cat /proc/sys/net/ipv4/tcp_max_syn_backlog
```
- 2 Open het bestand `/etc/sysctl.conf` in een teksteditor.
- 3 Stel de standaard wachtrijgrootte voor TCP backlog in door de volgende vermelding aan het bestand toe te voegen.

```
net.ipv4.tcp_max_syn_backlog=1280
```
- 4 Sla uw wijzigingen op en sluit het bestand.

ICMPv4-echo's naar uitzendadres weigeren

De aanbevolen beveiligingsprocedure is te verifiëren of de VMware-toepassing van uw hostmachine echoverzoeken van het ICMP-uitzendadres weigert.

Reacties op de uitzending van Internet Control Message Protocol (ICMP)-echo's vormen een aanvalsvector voor amplification-aanvallen en kunnen netwerktoewijzingen door schadelijke agenten mogelijk maken. Door uw toepassingshostmachines zo te configureren dat zij ICMPv4-echo's negeren, kunt u zich beschermen tegen dergelijke aanvallen.

Procedure

- 1 Voer de opdracht `# cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts` uit op de virtuele VMware-toepassingshostmachines om ze echoverzoeken van IPv4-uitzendadressen te laten weigeren.

Als de hostmachines zijn geconfigureerd om IPv4-omleidingen te weigeren, retourneert deze opdracht een waarde 0 voor `/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts`.
- 2 Als u een hostmachine voor een virtual appliance moet configureren om echoverzoeken van ICMPv4-uitzendadressen te weigeren, opent u het bestand `/etc/sysctl.conf` op de Windows-hostmachines in een teksteditor.
- 3 Zoek de vermelding `net.ipv4.icmp_echo_ignore_broadcasts=0`. Als de waarde voor deze vermelding niet is ingesteld op nul of als de vermelding niet bestaat, voegt u deze toe of werkt u de bestaande vermelding bij.
- 4 Sla de wijzigingen op en sluit het bestand.

IPv4-proxy ARP uitschakelen

Verifieer of IPv4-proxy ARP is uitgeschakeld (indien dit niet nodig is) op de hostmachine van uw VMware-toepassing om ongeautoriseerd delen van informatie te voorkomen.

Met IPv4-proxy ARP kan een systeem antwoorden versturen op ARP-verzoeken op één interface namens hosts die aangesloten zijn op een ander interface. Schakel deze instelling uit als u deze niet nodig hebt. Zo voorkomt u dat adresinformatie kan weglekken uit de gekoppelde netwerksegmenten.

Procedure

- 1 Voer de opdracht `# grep [01] /proc/sys/net/ipv4/conf/*/proxy_arp | egrep "default|all"` uit op de virtuele VMware-toepassingshostmachines om te bevestigen dat IPv4-proxy ARP is uitgeschakeld.

Als IPv6-proxy ARP is uitgeschakeld op de hostmachines, retourneert deze opdracht de waarde 0.

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

Als de hostmachines correct zijn geconfigureerd, is geen verdere actie nodig.

- 2 Als u IPv6-proxy ARP op hostmachines moet configureren, open dan het bestand `/etc/sysctl.conf` in een teksteditor.
- 3 Controleer de volgende vermeldingen.

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

Als deze vermeldingen niet bestaan of als hun waarde niet op nul is ingesteld, voegt u ze toe of werkt u de bestaande bij.

- 4 Sla gemaakte wijzigingen op en sluit het bestand.

IPv4 ICMP-omleidingsberichten weigeren

De aanbevolen beveiligingsprocedure is te verifiëren dat de virtuele VMware-toepassing van uw hostmachine IPv4 ICMP-omleidingsaanvragen weigert.

Routers maken gebruik van ICMP-omleidingsberichten om hosts te vertellen dat er een kortere route bestaat naar een bestemming. Een kwaadwillend ICMP-omleidingsbericht kan een man-in-the-middle-aanval mogelijk maken. Dergelijke berichten wijzigen de routeertabel van de host en zijn niet-geverifieerd. Zorg dat uw systeem zo is geconfigureerd dat dergelijke berichten worden genegeerd als zij niet op een andere manier nodig zijn.

Procedure

- 1 Voer de opdracht `# grep [01] /proc/sys/net/ipv4/conf/*/accept_redirects | egrep "default|all"` uit op de VMware-toepassingshostmachines om te bevestigen dat zij IPv4-omleidingsberichten weigeren.

Als de hostmachines zijn geconfigureerd om IPv4-omleidingen te weigeren, retourneert deze opdracht het volgende.

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

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

- 2 Als u een hostmachine voor een virtual appliance moet configureren om IPv4-omleidingsberichten te weigeren, opent u het bestand `/etc/sysctl.conf` in een teksteditor.

- 3 Controleer de waarden van de regels die beginnen met `net.ipv4.conf`.

Als de waarden voor de volgende vermeldingen niet zijn ingesteld op nul of als ze niet bestaan, voeg ze dan toe of werk de bestaande vermeldingen bij.

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

- 4 Sla uw wijzigingen op en sluit het bestand.

IPv6 ICMP-omleidingsberichten weigeren

De aanbevolen beveiligingsprocedure is te verifiëren dat de virtuele VMware-toepassing van uw hostmachine IPv6 ICMP-omleidingsaanvragen weigert.

Routers maken gebruik van ICMP-omleidingsberichten om hosts te vertellen dat er een kortere route bestaat naar een bestemming. Een kwaadwillend ICMP-omleidingsbericht kan een man-in-the-middle-aanval mogelijk maken. Dergelijke berichten wijzigen de routeertabel van de host en zijn niet-geverifieerd. Zorg dat uw systeem zo is geconfigureerd dat dergelijke berichten worden genegeerd als zij niet op een andere manier nodig zijn.

Procedure

- 1 Voer de opdracht `# grep [01] /proc/sys/net/ipv6/conf/*/accept_redirects | egrep "default|all"` uit op de hostmachines van de virtuele VMware-toepassing om te bevestigen dat zij IPv6-omleidingsberichten weigeren.

Als de hostmachines zijn geconfigureerd om IPv6-omleidingen te weigeren, retourneert deze opdracht het volgende.

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

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

- 2 Als u een hostmachine voor een virtual appliance moet configureren om IPv4-omleidingsberichten te weigeren, opent u het bestand `/etc/sysctl.conf` in een teksteditor.

- 3 Controleer de waarden van de regels die beginnen met `net.ipv6.conf`.

Als de waarden voor de volgende vermeldingen niet zijn ingesteld op nul of als ze niet bestaan, voeg ze dan toe of werk de bestaande vermeldingen bij.

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

- 4 Sla de wijzigingen op en sluit het bestand.

IPv4-martian-pakketten opslaan in logboek

De aanbevolen beveiligingsprocedure is te verifiëren of de virtuele VMware-toepassing van uw hostmachine IPv4-martian-pakketten in het logboek opslaat.

Martian-pakketten bevatten adressen waarvan het systeem weet dat ze ongeldig zijn. Configureer uw hostmachines zo dat ze deze berichten in het logboek opslaan, zodat u foute configuraties of lopende aanvallen kunt identificeren.

Procedure

- 1 Voer de opdracht `# grep [01] /proc/sys/net/ipv4/conf/*/log_martians | grep "default|all"` uit op de VMware-toepassing van uw hostmachines om te verifiëren of zij IPv4-martian-pakketten registreren.

Als de virtual machines zijn geconfigureerd om martian-pakketten te registreren, retourneert deze opdracht het volgende:

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

Als de hostmachines correct zijn geconfigureerd, is geen verdere actie nodig.

- 2 Als u virtual machines moet configureren voor het registreren van IPv4-martian-pakketten, opent u het bestand `/etc/sysctl.conf` in een teksteditor.
- 3 Controleer de waarden van de regels die beginnen met `net.ipv4.conf`.

Als de waarde voor de volgende vermeldingen niet is ingesteld op 1 of als ze niet bestaan, voeg ze dan toe aan het bestand of werk de bestaande vermeldingen bij.

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

- 4 Sla uw wijzigingen op en sluit het bestand.

Omgekeerde padfiltering van IPv4 gebruiken

De aanbevolen beveiligingsprocedure is te verifiëren of de virtual appliance VMware van hostmachines omgekeerde padfiltering van IPv4 gebruiken.

Omgekeerde padfiltering beschermt tegen vervalste bronadressen door ervoor te zorgen dat het systeem pakketten annuleert wanneer deze bronadressen hebben zonder route of met een route die niet naar de oorspronkelijke interface verwijst. Configureer uw hostmachines zodat deze zoveel mogelijk gebruikmaken van omgekeerde padfiltering. In bepaalde gevallen kan omgekeerde padfiltering ertoe leiden dat het systeem legitiem verkeer annuleert, afhankelijk van de systeemrol. In dat geval moet u wellicht een ruimere modus gebruiken of omgekeerde padfiltering helemaal uitschakelen.

Procedure

- 1 Voer de opdracht `# grep [01] /proc/sys/net/ipv4/conf/*/rp_filter | grep "default|all"` uit op de VMware-hostmachine van de virtual appliance om te controleren of omgekeerde padfiltering van IPv4 wordt gebruikt.

Als de virtual machines omgekeerde padfiltering van IPv4 gebruiken, geeft deze opdracht het volgende resultaat:

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

Als uw virtual machines correct zijn geconfigureerd, is geen verdere actie nodig.

- 2 Als u omgekeerde padfiltering van IPv4 moet configureren op hostmachines, opent u het bestand `/etc/sysctl.conf` in een teksteditor.
- 3 Controleer de waarden van de regels die beginnen met `net.ipv4.conf`.

Als de waarden voor de volgende vermeldingen niet zijn ingesteld op 1 of als ze niet bestaan, voeg ze dan toe aan het bestand of werk de bestaande vermeldingen bij.

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

- 4 Sla de wijzigingen op en sluit het bestand.

IPv4-forwarding weigeren

Verifieer of de VMware-toepassing van uw hostmachines de IPv4-forwarding weigeren.

Als het systeem is geconfigureerd voor IP-forwarding en geen toegewezen router is, kunnen aanvallers het gebruiken om de netwerkbeveiliging te omzeilen door een pad voor communicatie aan te bieden dat niet wordt gefilterd door netwerkapparaten. Om dit risico te vermijden, configureert u de hostmachines van uw virtual appliance zo dat IPv4-forwarding wordt geweigerd.

Procedure

- 1 Voer de opdracht `# cat /proc/sys/net/ipv4/ip_forward` uit op de VMware-toepassing van uw hostmachines om te bepalen dat zij IPv4-forwarding weigeren.

Als de hostmachines zijn geconfigureerd om IPv4-forwarding te weigeren, retourneert deze opdracht een waarde 0 voor `/proc/sys/net/ipv4/ip_forward`. Als de virtual machines correct zijn geconfigureerd, is geen verdere actie nodig.

- 2 Als u een hostmachine voor een virtual appliance moet configureren om IPv4-forwarding te weigeren, opent u het bestand `/etc/sysctl.conf` in een teksteditor.
- 3 Zoek de vermelding `net.ipv4.ip_forward=0`. Als de waarde voor deze vermelding op dit moment niet is ingesteld op nul of als de vermelding niet bestaat, voegt u deze toe of werkt u de bestaande vermelding bij.
- 4 Sla gemaakte wijzigingen op en sluit het bestand.

IPv6-forwarding weigeren

De aanbevolen beveiligingsprocedure is te verifiëren of de VMware-toepassing van uw hostsysteem IPv6-forwarding weigert.

Als het systeem is geconfigureerd voor IP-forwarding en geen toegewezen router is, kunnen aanvallers het gebruiken om de netwerkbeveiliging te omzeilen door een pad voor communicatie aan te bieden dat niet wordt gefilterd door netwerkapparaten. Om dit risico te vermijden, configureert u de hostmachines van uw virtual appliance zo dat IPv6-forwarding wordt geweigerd.

Procedure

- 1 Voer de opdracht `# grep [01] /proc/sys/net/ipv6/conf/*/forwarding | grep "default|all"` uit op de VMware-toepassing van uw hostmachines om te verifiëren of zij IPv6-forwarding weigeren.

Als de hostmachines zijn geconfigureerd om IPv6-forwarding te weigeren, retourneert deze opdracht het volgende:

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

Als de hostmachines correct zijn geconfigureerd, is geen verdere actie nodig.

- 2 Als u een hostmachine moet configureren om IPv6-forwarding te weigeren, opent u het bestand `/etc/sysctl.conf` in een teksteditor.
- 3 Controleer de waarden van de regels die beginnen met `net.ipv6.conf`.

Als de waarden voor de volgende vermeldingen niet zijn ingesteld op nul of als ze niet bestaan, voeg ze dan toe of werk de bestaande vermeldingen bij.

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

- 4 Sla gemaakte wijzigingen op en sluit het bestand.

IPv4 TCP Syncookies gebruiken

Controleer of de hostmachines van uw VMware-toepassingen gebruik maken van IPv4 TCP Syncookies.

Een TCP SYN flood-aanval kan een denial of service veroorzaken door de TCP-verbindingstabel van een systeem te vullen met verbindingen in de SYN_RCVD-status. Syncookies voorkomen het traceren van een verbinding tot ontvangst van een daarop volgende ACK die verifieert dat de andere partij een geldige verbinding probeert te maken en geen flood-aanval wil starten. Deze techniek werkt niet in volledige overeenstemming met standaarden, maar wordt alleen geactiveerd tijdens een flood-conditie, en maakt verdediging van het systeem mogelijk terwijl de service voor geldige verzoeken blijft doorlopen.

Procedure

- 1 Voer de opdracht `# cat /proc/sys/net/ipv4/tcp_syncookies` uit op de VMware-toepassingshostmachines om te controleren of ze IPv4 TCP Syncookies gebruiken.

Als de hostmachines geconfigureerd zijn om IPv4 doorsturen te weigeren, geeft deze opdracht een waarde van 1 voor `/proc/sys/net/ipv4/tcp_syncookies`. Als de virtual machines correct zijn geconfigureerd, is geen verdere actie nodig.

- 2 Als u een virtual appliance moet configureren voor het gebruik van IPv4 TCP Syncookies, open dan `/etc/sysctl.conf` in een teksteditor.

- 3 Zoek de vermelding `net.ipv4.tcp_syncookies=1`.

Als de waarde voor deze vermelding op dit moment niet is ingesteld op 1 of als de vermelding niet bestaat, voegt u deze toe of werkt u de bestaande vermelding bij.

- 4 Sla gemaakte wijzigingen op en sluit het bestand.

IPv6-router-advertisements weigeren

Verifieer of de VMware-toepassing van uw hostmachine informatie over het accepteren van router-advertisements en ICMP-omleidingen weigert, tenzij anderszins is vereist voor de systeembewerking.

Met IPv6 kunnen systemen hun netwerkapparaten configureren door automatisch informatie van het netwerk te gebruiken. Vanuit een veiligheidsperspectief wordt de voorkeur gegeven aan handmatig configureren van belangrijke configuratie-informatie boven het accepteren van deze informatie van het netwerk zonder verificatie.

Procedure

- 1 Voer de opdracht `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra | egrep "default|all"` uit op de VMware-toepassing van uw hostmachines om te verifiëren of zij router-advertisements weigeren.

Als de hostmachines zijn geconfigureerd om IPv6-router-advertisements te weigeren, retourneert deze opdracht de waarde 0:

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

Als de hostmachines correct zijn geconfigureerd, is geen verdere actie nodig.

- 2 Als u een hostmachine moet configureren om IPv6-router-advertisements te weigeren, opent u het bestand `/etc/sysctl.conf` in een teksteditor.
- 3 Controleer de volgende vermeldingen.

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

Als deze vermeldingen niet bestaan of als hun waarde niet is ingesteld op nul, voegt u de vermeldingen toe of werkt u de bestaande bij.

- 4 Sla gemaakte wijzigingen op en sluit het bestand.

IPv6-routeraanvragen weigeren

De aanbevolen beveiligingsprocedure is te verifiëren dat de VMware-toepassing van uw hostmachine IPv6-routeraanvragen weigert tenzij anderszins vereist voor de systeembewerking.

De instelling routeraanvragen bepaalt hoeveel routeraanvragen worden verzonden als de interface wordt geladen. Als de adressen statisch zouden zijn toegewezen, is het niet nodig een aanvraag te sturen.

Procedure

- 1 Voer de opdracht `# grep [01] /proc/sys/net/ipv6/conf/*/router_sollicitations | grep "default|all"` uit op de VMware-toepassing van uw hostmachines om te verifiëren of zij IPv6-routeraanvragen weigeren.

Als de hostmachines zijn geconfigureerd om IPv6-routeraankondigingen te weigeren, retourneert deze opdracht het volgende:

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

Als de hostmachines correct zijn geconfigureerd, is geen verdere actie nodig.

- 2 Als u een hostmachine moet configureren om IPv6-routeraanvragen te weigeren, opent u het bestand `/etc/sysctl.conf` in een teksteditor.
- 3 Controleer de volgende vermeldingen.

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

Als deze vermeldingen niet bestaan of als hun waarde niet op nul is ingesteld, voegt u ze toe of werkt u de bestaande bij.

- 4 Sla gemaakte wijzigingen op en sluit het bestand.

IPv6-routervoorkeuren in routeraanvragen weigeren

Verifieer of de VMware-toepassing van uw hostmachine IPv6-routeraanvragen weigert tenzij anderszins is vereist voor de systeembewerking.

De routervoorkeur in de aanvraaginstelling bepaalt de routervoorkeuren. Als de adressen statisch zouden zijn toegewezen, is het niet nodig om routervoorkeuren voor aanvragen te ontvangen.

Procedure

- 1 Voer de opdracht `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_rtr_pref | egrep "default|all"` uit op de VMware-toepassing van uw hostmachines om te verifiëren of zij IPv6-routeraanvragen weigeren.

Als de hostmachines zijn geconfigureerd om IPv6-routeraankondigingen te weigeren, retourneert deze opdracht het volgende:

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

Als de hostmachines correct zijn geconfigureerd, is geen verdere actie nodig.

- 2 Als u een hostmachine moet configureren om IPv6-routeraanvragen te weigeren, opent u het bestand `/etc/sysctl.conf` in een teksteditor.
- 3 Controleer de volgende vermeldingen.

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

Als de vermeldingen niet bestaan of als hun waarde niet is ingesteld op nul, voegt u de vermeldingen toe of werkt u de bestaande bij.

- 4 Sla gemaakte wijzigingen op en sluit het bestand.

IPv6-routervoorvoegsels weigeren

Verifieer dat de VMware-toepassing van uw hostmachine informatie over IPv6-routervoorvoegsels weigert tenzij anderszins is vereist voor de systeembewerking.

De instelling `accept_ra_pinfo` regelt of het systeem informatie over voorvoegsels van de router accepteert. Als de adressen statisch zouden zijn toegewezen, is het niet nodig om informatie over routervoorvoegsels te ontvangen.

Procedure

- 1 Voer de opdracht `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_pinfo | egrep "default|all"` uit op de VMware-toepassing van uw hostmachines om te verifiëren dat zij informatie over voorvoegsels van de IPv6-router weigeren.

Als de hostmachines zijn geconfigureerd om IPv6-routeraankondigingen te weigeren, retourneert deze opdracht het volgende.

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

Als de hostmachines correct zijn geconfigureerd, is geen verdere actie nodig.

- 2 Als u hostmachines moet configureren zodat ze informatie over IPv6-routervoorvoegsels weigeren, opent u het bestand `/etc/sysctl.conf` in een teksteditor.
- 3 Controleer de volgende vermeldingen.

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

Als deze vermeldingen niet bestaan of als hun waarde niet op nul is ingesteld, voegt u ze toe of werkt u de bestaande bij.

- 4 Sla gemaakte wijzigingen op en sluit het bestand.

Hop-limit-instellingen van IPv6-router-advertisement weigeren

Verifieer of de VMware-toepassing van uw hostmachines de hop-limit-instellingen voor de IPv6-router weigert (tenzij deze nodig zijn).

De instelling `accept_ra_defrtr` regelt of het systeem hop-limit-instellingen accepteert van een router-advertisement. Door deze in te stellen op nul, voorkomt u dat een router uw standaard IPv6-hop-limit-instelling voor uitgaande pakketten wijzigt.

Procedure

- 1 Voer de opdracht `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_defrtr | egrep "default|all"` uit op de VMware-toepassing van uw hostmachines om te verifiëren of zij de hop-limit-instellingen voor de IPv6-router weigeren.

Als de hostmachines zijn geconfigureerd om hop-limit-instellingen voor IPv6 te weigeren, retourneert deze opdracht de waarden 0.

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

Als de hostmachines correct zijn geconfigureerd, is geen verdere actie nodig.

- 2 Als u een hostmachine moet configureren om hop-limit-instellingen voor IPv6-routes te weigeren, opent u het bestand `/etc/sysctl.conf` in een teksteditor.
- 3 Controleer de volgende vermeldingen.

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

Als deze vermeldingen niet bestaan of als hun waarde niet op nul is ingesteld, voegt u ze toe of werkt u de bestaande bij.

- 4 Sla gemaakte wijzigingen op en sluit het bestand.

Autoconf-instellingen voor IPv6-router-advertisement weigeren

Verifieer of de VMware-toepassing van uw hostmachines de autoconf-instellingen voor de IPv6-router weigert (tenzij deze nodig zijn).

De instelling `autoconf` regelt of router-advertisements ertoe kunnen leiden dat het systeem een globaal unicast-adres toewijst aan een interface.

Procedure

- 1 Voer de opdracht `# grep [01] /proc/sys/net/ipv6/conf/*/autoconf | egrep "default|all"` uit op de VMware-toepassing van uw hostmachines om te verifiëren dat zij de `autoconf`-instellingen voor de IPv6-router weigeren.

Als de hostmachines zijn geconfigureerd om `autoconf`-instellingen voor IPv6 te weigeren, retourneert deze opdracht de waarde 0.

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

Als de hostmachines correct zijn geconfigureerd, is geen verdere actie nodig.

- 2 Als u een hostmachine moet configureren om `autoconf`-instellingen voor IPv6-routes te weigeren, opent u het bestand `/etc/sysctl.conf` in een teksteditor.
- 3 Controleer de volgende vermeldingen.

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

Als deze vermeldingen niet bestaan of als hun waarde niet op nul is ingesteld, voegt u ze toe of werkt u de bestaande bij.

- 4 Sla gemaakte wijzigingen op en sluit het bestand.

IPv6-neighbor-aanvragen weigeren

Verifieer dat de VMware-toepassing van uw hostmachines IPv6-neighbor-aanvragen weigert, tenzij deze noodzakelijk zijn.

De instelling `dad_transmits` bepaalt hoeveel neighbor-aanvragen per adres verzonden moeten worden (globaal en linklokaal) als een interface wordt geladen, om te garanderen dat het gewenste adres uniek op het netwerk is.

Procedure

- 1 Voer de opdracht `# grep [01] /proc/sys/net/ipv6/conf/*/dad_transmits | egrep "default|all"` uit op de VMware-toepassing van uw hostmachines om te verifiëren dat zij IPv6-neighbor-aanvragen weigeren.

Als de hostmachines zijn geconfigureerd om IPv6-neighbor-aanvragen te weigeren, retourneert deze opdracht de waarde 0.

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

Als de hostmachines correct zijn geconfigureerd, is geen verdere actie nodig.

- 2 Als u een hostmachine moet configureren om IPv6-neighbor-aanvragen te weigeren, opent u het bestand `/etc/sysctl.conf` in een teksteditor.
- 3 Controleer de volgende vermeldingen.

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

Als deze vermeldingen niet bestaan of als hun waarde niet op nul is ingesteld, voegt u ze toe of werkt u de bestaande bij.

- 4 Sla gemaakte wijzigingen op en sluit het bestand.

Max. aantal IPv6-adressen beperken

Controleer of de hostmachines van uw VMware-toepassing max. IPv6-adresinstellingen beperkt tot het minimaal vereiste voor systeemgebruik.

De maximale adresinstellingen bepalen hoeveel algemene unicast IPv6-adressen beschikbaar zijn voor ieder interface. De standaard is 16, maar u moet dit instellen tot precies het aantal statisch geconfigureerde algemene adressen die benodigd zijn voor uw systeem.

Procedure

- 1 Voer de opdracht `# grep [1] /proc/sys/net/ipv6/conf/*/max_addresses | egrep "default|all"` uit op de hostmachines van de VMware-toepassingen om te controleren of ze het max. aantal IPv6-adressen correct beperken.

Als de hostmachines geconfigureerd zijn om het maximumaantal IPv6-adressen te beperken, geeft deze opdracht de waarde 1 als resultaat.

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

Als de hostmachines correct zijn geconfigureerd, is geen verdere actie nodig.

- 2 Als u het max. IPv6-adressen moet configureren op hostmachines, open dan het bestand `/etc/sysctl.conf` in een teksteditor.
- 3 Controleer de volgende vermeldingen.

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

Als deze vermeldingen niet bestaan of als hun waarde niet op 1 is ingesteld, voegt u ze toe of werkt u de bestaande bij.

- 4 Sla gemaakte wijzigingen op en sluit het bestand.

Netwerkinstellingen voor de Infrastructure as a Service-host configureren

Om veiligheidsredenen raden wij u aan de netwerkcommunicatie-instellingen op uw VMware-hostmachine voor uw Infrastructure as a Service-onderdeel (IaaS) te configureren volgens de vereisten en richtlijnen van VMware.

Configureer de netwerkconfiguratie van de Infrastructure as a Service-hostmachine (IaaS) zodat deze alle vRealize Automation-functies inclusief bijbehorende beveiliging ondersteunt.

Zie [Het onderdeel Infrastructure as a Service beveiligen](#).

Poorten en protocollen configureren

Als best practice voor beveiliging, moet u de poorten en protocollen voor alle vRealize Automation-toepassingen en -onderdelen configureren conform de VMware-richtlijnen.

Configureer inkomende en uitgaande poorten voor vRealize Automation-onderdelen zoals vereist voor kritieke systeemonderdelen om te kunnen functioneren in productie. Schakel alle niet-gebruikte poorten en protocollen uit. Zie *vRealize Automation Referentie-architectuur* in de [documentatie voor VMware vRealize Automation](#).

Hulpprogramma voor poorten en protocollen

Met het hulpprogramma voor poorten en protocollen kunt u poortinformatie voor een variëteit en een combinatie van VMware-producten weergeven op één dashboard. U kunt ook geselecteerde gegevens uit het hulpprogramma exporteren voor offline toegang. Het hulpprogramma voor poorten en protocollen ondersteunt momenteel:

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

Het hulpprogramma is beschikbaar op <https://ports.vmware.com/>.

Voor gebruikers verplichte poorten

Configureer als best practice voor de beveiliging vRealize Automation gebruikerspoorten conform de VMware-richtlijnen.

Zorg dat u vereiste poorten alleen opent via een beveiligd netwerk.

SERVER	POORTEN
vRealize Automation-toepassing	443, 8443

Voor beheerders vereiste poorten

De aanbevolen beveiligingsprocedure is de vRealize Automation-beheerderspoorten te configureren in overeenstemming met de VMware-richtlijnen.

Zorg dat u vereiste poorten alleen opent via een beveiligd netwerk.

SERVER	POORTEN
vRealize Application Services-server	5480

vRealize Automation-toepassingspoorten

Configureer als best practice voor de beveiliging inkomende en uitgaande poorten voor de vRealize Automation-toepassing conform de aanbevelingen van VMware.

Inkomende poorten

Configureer het minimaal aantal vereiste inkomende poorten voor de vRealize Automation-toepassing. Configureer optionele poorten indien nodig voor uw systeemconfiguratie.

Tabel 8-1. Minimaal vereiste inkomende poorten

POORT	PROTOCOL	OPMERKINGEN
443	TCP	Toegang tot de vRealize Automation-console en API-oproepen.
8443	TCP	VMware Remote Console-proxy.
5480	TCP	Toegang tot de beheerinterface van de vRealize Automation-toepassing.
5488, 5489	TCP	Intern. Gebruikt door de vRealize Automation-toepassing voor updates.
5672	TCP	RabbitMQ-berichten. Opmerking Als u vRealize Automation-toepassing-instanties clustert, kan het zijn dat u de open poorten 4369 en 25672 moet configureren.
40002	TCP	Benodigd voor vIDM-service. Hier bevindt zich een firewall voor alle externe verkeer, met uitzondering van verkeer van andere vRealize Automation-toepassing-knooppunten indien toegevoegd aan een HA-configuratie.

Configureer indien nodig optionele inkomende poorten.

Tabel 8-2. Optionele inkomende poorten

POORT	PROTOCOL	OPMERKINGEN
22	TCP	(Optionele) SSH. Schakel in een productie-omgeving de SSH-service die luistert op poort 22 uit en sluit poort 22.
80	TCP	(Optionele) omleiding naar 443.

Uitgaande poorten

Configureer de vereiste uitgaande poorten.

Tabel 8-3. Configureer de minimaal vereiste uitgaande poorten.

POORT	PROTOCOL	OPMERKINGEN
25.587	TCP, UDP	SMTP voor het verzenden van uitgaande e-mails.
53	TCP, UDP	DNS.
67, 68, 546, 547	TCP, UDP	DHCP.
110, 995	TCP, UDP	POP voor het ontvangen van inkomende e-mails.
143, 993	TCP, UDP	IMAP voor het ontvangen van inkomende e-mails.
443	TCP	Infrastructure as a Service Manager Service over HTTPS.

Configureer indien nodig optionele uitgaande poorten.

Tabel 8-4. Optionele uitgaande poorten.

POORT	PROTOCOL	OPMERKINGEN
80	TCP	(Optioneel) Voor het ophalen van software-updates. U kunt updates afzonderlijk downloaden en toepassen.
123	TCP, UDP	(Optioneel) Voor het maken van directe verbinding met NTP, in plaats van tijd van de host te gebruiken.

Hulpprogramma voor poorten en protocollen

Met het hulpprogramma voor poorten en protocollen kunt u poortinformatie voor een variëteit en een combinatie van VMware-producten weergeven op één dashboard. U kunt ook geselecteerde gegevens uit het hulpprogramma exporteren voor offline toegang. Het hulpprogramma voor poorten en protocollen ondersteunt momenteel:

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

Het hulpprogramma is beschikbaar op <https://ports.vmware.com/>.

Infrastructure as a Service-poorten

Om veiligheidsredenen raden wij u aan inkomende en uitgaande poorten voor de Infrastructure as a Service (IaaS)-onderdelen te configureren volgens de VMware-richtlijnen.

Inkomende poorten

Configureer de minimaal vereiste inkomende poorten voor de IaaS-onderdelen.

Tabel 8-5. Minimaal vereiste inkomende poorten

ONDERDEEL	POORT	PROTOCOL	OPMERKINGEN
Manager Service	443	TCP	Communicatie met IaaS-onderdelen en de vRealize Automation-toepassing via HTTPS. Voor alle virtualisatiehosts die proxyagenten beheren, moet ook de TCP-poort 443 geopend zijn voor inkomend verkeer.

Uitgaande poorten

Configureer de minimaal vereiste uitgaande poorten voor de IaaS-onderdelen.

Tabel 8-6. Configureer de minimaal vereiste uitgaande poorten.

ONDERDEEL	POORT	PROTOCOL	OPMERKINGEN
Alles	53	TCP, UDP	DNS.
Alles		TCP, UDP	DHCP.
Manager Service	443	TCP	Communicatie met de vRealize Automation-toepassing via HTTPS.
Website	443	TCP	Communicatie met Manager Service via HTTPS.
Distributed Execution Managers	443	TCP	Communicatie met Manager Service via HTTPS.
Proxyagenten	443	TCP	Communicatie met Manager Service en virtualisatiehosts via HTTPS.
Gastagent	443	TCP	Communicatie met Manager Service via HTTPS.
Managerservice, website	1433	TCP	MSSQL.

Configureer, indien nodig, optionele uitgaande poorten.

Tabel 8-7. Optionele uitgaande poorten.

ONDERDEEL	POORT	PROTOCOL	OPMERKINGEN
Alles	123	TCP, UDP	NTP is optioneel

Audits en logboekregistratie

De aanbevolen beveiligingsprocedure is audits en logboekregistratie in te stellen op uw vRealize Automation-systeem in overeenstemming met VMware-aanbevelingen.

Met externe logboekregistratie op een centrale logboekhost kunnen logboekbestanden veilig worden opgeslagen. Door logboekbestanden op een centrale logboekhost te verzamelen, kunt u de omgeving met één hulpmiddel controleren. U kunt daarnaast aggregaatanalyse uitvoeren en naar bewijs zoeken van bedreigingen zoals gecoördineerde aanvallen op meerdere entiteiten binnen de infrastructuur. Door logboekregistratie op een beveiligde, centrale logboekhost uit te voeren, kunt u voorkomen dat er met logboeken wordt geknoeid. Bovendien beschikt u hiermee over een controlerecord over langere tijd.

Controleren of de externe logboekserver is beveiligd

Wanneer hackers door de beveiliging van uw hostmachine zijn gekomen, proberen zij vaak logboekbestanden te vinden zodat zij deze kunnen bewerken om hun sporen te wissen en de controle te behouden zonder te worden ontdekt. Door de externe logboekserver te beveiligen helpt u geknoei met logboeken te ontmoedigen.

Een geautoriseerde NTP-server gebruiken

Controleer of alle hostmachines dezelfde relatieve tijdsbron gebruiken, inclusief de relevante lokalisatie-offset, en dat u de relatieve tijdsbron kunt relateren aan een vooraf afgesproken tijd, zoals Coordinated Universal Time (UTC). Door een gedisciplineerde benadering van tijdsbronnen kunt u snel de acties van een indringer volgen en correlaties zoeken wanneer u de relevante logboekbestanden bekijkt. Onjuiste tijdsinstellingen maken het moeilijk inspectie en correlatie van logboekbestanden uit te voeren om aanvallen te detecteren en kunnen audits onnauwkeurig maken.

Gebruik ten minste drie NTP-servers van externe tijdsbronnen of configureer een paar lokale NTP-servers op een vertrouwd netwerk die hun tijd van ten minste drie externe tijdsbronnen krijgen.